

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-036015

(43)Date of publication of application : 02.02.2000

(51)Int.Cl. G06K 17/00
G06K 19/07
G06K 19/073
G09C 1/00
H04L 9/36

(21)Application number : 10-203399

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 17.07.1998

(72)Inventor : NISHIOKA MITSURU

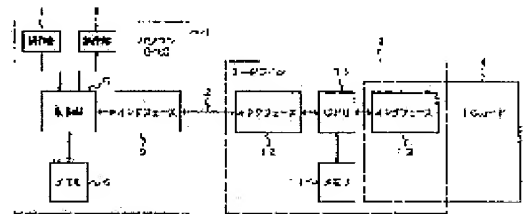
(54) IC CARD PROCESSOR, IC CARD, IC CARD PROCESSING SYSTEM AND IC CARD PROCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the leak of information concerning an issuing command and to attain improvement in the security of an IC card concerning issuing processing by hiding the telegraphic message of the issuing command to an issuing object card with a means such as enciphering.

SOLUTION: A control part 5 has an enciphering function for enciphering the telegraphic message of a command while using a production number (card peculiar information) supplied from an IC card 4 as a cryptographic key. At the time of card production, all the IC cards 4 have the same decoding logic and decoding key and on the side of a personal computer(PC) 1 for transmitting the telegraphic message of the command to the IC card 4, the correspondent encoding logic and cryptographic key are provided as well. Namely, in primary issuing processing, the same decoding logic (program) and key (decoding key) are used for all the IC cards 4 in order to create a file common for each

system. In this case, the telegraphic message of the enciphered command gets equal for all the IC cards 4 but a 'command' in naked state can be hidden at least.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-36015

(P2000-36015A)

(43) 公開日 平成12年2月2日 (2000.2.2)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	B 5 B 0 3 5
			D 5 B 0 5 8
19/07		G 0 9 C 1/00	6 6 0 A 5 K 0 1 3
19/073		G 0 6 K 19/00	N
G 0 9 C 1/00	6 6 0		P
審査請求 未請求 請求項の数17 O L (全 33 頁) 最終頁に続く			

(21) 出願番号 特願平10-203399

(22) 出願日 平成10年7月17日 (1998.7.17)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 西岡 満

神奈川県川崎市幸区柳町70番地 東芝ソシ

オエンジニアリング株式会社内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B035 AA13 BB09 CA38

5B058 CA01 KA35 YA20

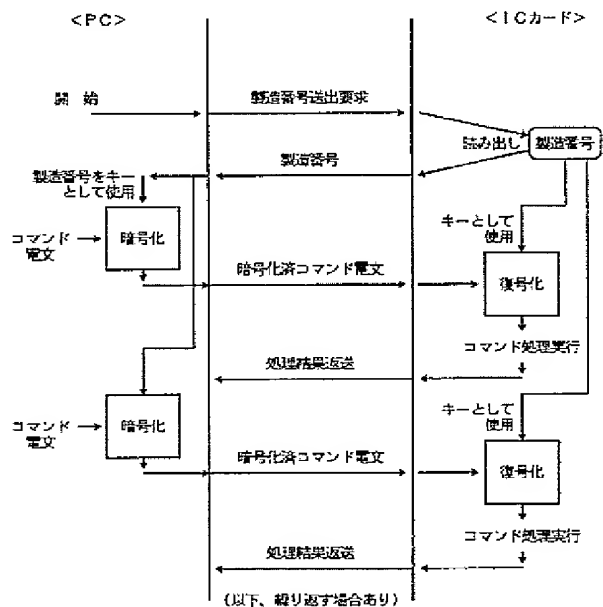
5K013 BA02 CA01 EA00 EA06 FA03

(54) 【発明の名称】 ICカード処理装置とICカードとICカード処理システムとICカード処理方法

(57) 【要約】

【課題】 この発明は、発行対象のICカードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関するICカードのセキュリティを向上させることができる。

【解決手段】 この発明は、発行対象のICカードに対する発行コマンド電文を暗号化等の手段により隠蔽するようにしたものである。



【特許請求の範囲】

【請求項 1】 ICカードへ送信するコマンド電文を生成する生成手段と、

ICカードに対してカード固有番号の出力要求を上記 ICカードへ送信する第 1 の送信手段と、

この第 1 の送信手段に应答して得られる ICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、

この暗号化手段により暗号化されたコマンド電文を上記 ICカードへ送信する第 2 の送信手段と、

この第 2 の送信手段に应答して得られる処理結果に応じて処理を終了する終了手段と、

を具備したことを特徴とする ICカード処理装置。

【請求項 2】 カード固有番号を記憶している記憶手段と、

外部装置からのカード固有番号の出力要求に应答して上記記憶手段から読出したカード固有番号を上記外部装置へ送信する第 1 の送信手段と、

この第 1 の送信手段に应答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段と、

この処理手段による処理結果を上記外部装置へ送信する第 2 の送信手段と、

を具備したことを特徴とする ICカード。

【請求項 3】 ICカード処理装置と ICカードとからなる ICカード処理システムにおいて、

上記 ICカード処理装置が、

ICカードへ送信するコマンド電文を生成する生成手段と、

ICカードに対してカード固有番号の出力要求を上記 ICカードへ送信する第 1 の送信手段と、

この第 1 の送信手段に应答して得られる ICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、

この暗号化手段により暗号化されたコマンド電文を上記 ICカードへ送信する第 2 の送信手段とからなり、

上記 ICカードが、

カード固有番号を記憶している記憶手段と、

上記 ICカード処理装置からのカード固有番号の出力要求に应答して上記記憶手段から読出したカード固有番号を上記 ICカード処理装置へ送信する第 3 の送信手段と、

この第 3 の送信手段に应答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、

ことを特徴とする ICカード処理システム。

【請求項 4】 ICカード処理装置と ICカードとからなる ICカード処理システムにおいて、

上記 ICカード処理装置が、

ICカードへ送信するコマンド電文を生成する生成手段と、

ICカードに対してカード固有番号の出力要求を上記 ICカードへ送信する第 1 の送信手段と、

この第 1 の送信手段に应答して得られる ICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、

この暗号化手段により暗号化されたコマンド電文を上記 ICカードへ送信する第 2 の送信手段と、

この第 2 の送信手段に应答して得られる処理結果が供給された際に、上記生成手段により生成されたコマンド電文の送信を行うか終了するかを判断する判断手段と、

この判断手段によりコマンド電文の送信を判断した際に、上記 ICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を上記暗号化手段により暗号化し、上記第 2 の送信手段により暗号化されたコマンド電文を上記 ICカードへ送信する第 1 の処理手段とからなり、

上記 ICカードが、

カード固有番号を記憶している記憶手段と、

上記 ICカード処理装置からのカード固有番号の出力要求に应答して上記記憶手段から読出したカード固有番号を上記 ICカード処理装置へ送信する第 3 の送信手段と、

この第 3 の送信手段に应答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う第 2 の処理手段と、

この第 2 の処理手段による処理結果を上記 ICカード処理装置へ送信する第 4 の送信手段とからなる、

ことを特徴とする ICカード処理システム。

【請求項 5】 ICカード処理装置と ICカードとからなる ICカード処理システムにおいて、

上記 ICカード処理装置が、

ICカードへ送信するコマンド電文を生成する第 1 の生成手段と、

ICカードに対して乱数の出力要求を上記 ICカードへ送信する第 1 の送信手段と、

この第 1 の送信手段に应答して得られる ICカードからの乱数を暗号キーとして上記第 1 の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、

この暗号化手段により暗号化されたコマンド電文を上記 ICカードへ送信する第 2 の送信手段とからなり、

上記 ICカードが、

カード固有番号を記憶している記憶手段と、

この記憶手段から読出したカード固有番号に基づく乱数

を生成する第 2 の生成手段と、
上記 IC カード処理装置からの乱数の出力要求に回答して上記第 2 の生成手段により生成された乱数を上記 IC カード処理装置へ送信する第 3 の送信手段と、
この第 3 の送信手段に回答して得られる暗号化されたコマンド電文を上記第 2 の生成手段により生成された乱数を復号キーとして復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とする IC カード処理システム。

【請求項 6】 IC カード処理装置と IC カードとからなる IC カード処理システムにおいて、
上記 IC カード処理装置が、
前回の乱数を記憶する記憶手段と、
この記憶手段により読出した前回の乱数に基づく乱数を生成する第 1 の生成手段と、
IC カードへ送信するコマンド電文を生成する第 2 の生成手段と、
上記第 1 の生成手段により生成された乱数を上記 IC カードへ送信する第 1 の送信手段と、
この第 1 の送信手段に回答して得られる IC カードからの処理準備開始応答が供給された際に、上記第 1 の生成手段により生成された乱数を暗号キーとして上記第 2 の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記 IC カードへ送信する第 2 の送信手段と、
この第 2 の送信手段に回答して得られる IC カードからの応答が供給された際に、上記第 1 の生成手段により生成された乱数を暗号キーとして上記第 2 の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記 IC カードへ上記第 2 の送信手段で送信する第 1 の処理手段とからなり、
上記 IC カードが、
上記 IC カード処理装置からの乱数に基づいて、処理準備開始応答を上記 IC カード処理装置へ送信する上記第 3 の送信手段と、
上記 IC カード処理装置からの乱数に基づいて、上記第 3 の送信手段に回答して得られる暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う第 2 の処理手段と、
この第 2 の処理手段による処理結果を上記 IC カード処理装置へ送信する第 4 の送信手段と、
この第 4 の送信手段に回答して得られる暗号化されたコマンド電文を、上記復号化手段で上記 IC カード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第 2 の処理手段で行う第 3 の処理手段とからなる、

ことを特徴とする IC カード処理システム。

【請求項 7】 IC カード処理装置と IC カードと IC カードとからなる IC カード処理システムにおいて、
上記 IC カードが、
上記 IC カード処理装置から与えられる前回処理に使用された乱数を記憶する第 1 の記憶手段と、
認証データとを記憶する第 2 の記憶手段と、
上記 IC カード処理装置からの認証データと上記第 2 の記憶手段に記憶されている認証データとが一致した際に、上記第 1 の記憶手段に記憶されている前回の乱数を上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、
上記 IC カード処理装置が、
上記 IC カードへ認証データを送信する第 2 の送信手段と、
この第 2 の送信手段に回答して上記 IC カードから得られる前回の乱数に基づく乱数を生成する第 1 の生成手段と、
この第 1 の生成手段で生成された乱数を上記 IC カードへ送信する第 3 の送信手段と、
IC カードへ送信するコマンド電文を生成する第 2 の生成手段と、
上記第 1 の生成手段により生成された乱数を上記 IC カードへ送信する第 4 の送信手段と、
この第 4 の送信手段に回答して得られる IC カードからの処理準備開始応答が供給された際に、上記第 1 の生成手段により生成された乱数を暗号キーとして上記第 2 の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記 IC カードへ送信する第 5 の送信手段と、
この第 5 の送信手段に回答して得られる IC カードからの応答が供給された際に、上記第 1 の生成手段により生成された乱数を暗号キーとして上記第 2 の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記 IC カードへ上記第 5 の送信手段で送信する第 1 の処理手段とからなり、
上記 IC カードが、
上記 IC カード処理装置からの乱数に基づいて、処理準備開始応答を上記 IC カード処理装置へ送信する上記第 6 の送信手段と、
上記 IC カード処理装置からの乱数に基づいて、上記第 6 の送信手段に回答して得られる暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う第 2 の処理手段と、
この第 2 の処理手段による処理結果を上記 IC カード処理装置へ送信する第 7 の送信手段と、
この第 7 の送信手段に回答して得られる暗号化されたコ

マンド電文を、上記復号化手段で上記 IC カード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第 2 の処理手段で行う第 3 の処理手段とからなる、

ことを特徴とする IC カード処理システム。

【請求項 8】 IC カード処理装置と IC カードとキーカードとからなる IC カード処理システムにおいて、上記キーカードが、

指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドを記憶する第 1 の記憶手段と、

上記 IC カード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第 1 の記憶手段から読出し、この読出したコマンドを上記 IC カード処理装置からの暗号キーに基づいて暗号化する暗号化手段と、

この暗号化手段により暗号化した暗号化済みコマンドを上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、

上記 IC カード処理装置が、

上記 IC カードに対してカード固有番号の出力要求を送信する第 1 の送信手段と、

上記キーカードへ指定コマンド番号と実行パラメータと上記第 1 の送信手段に回答して得られる IC カードのカード固有番号としての暗号キーを送信する第 2 の送信手段と、

この第 2 の送信手段に回答して上記キーカードから得られる暗号化済みコマンドを上記 IC カードへ送信する第 3 の送信手段とからなり、

上記 IC カードが、

カード固有番号を記憶している第 2 の記憶手段と、

上記 IC カード処理装置からのカード固有番号の出力要求に回答して上記第 2 の記憶手段から読出したカード固有番号を上記 IC カード処理装置へ送信する第 3 の送信手段と、

この第 3 の送信手段に回答して得られる暗号化されたコマンド電文を上記第 2 の記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、

ことを特徴とする IC カード処理システム。

【請求項 9】 IC カード処理装置と IC カードとキーカードとからなる IC カード処理システムにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第 1 の記憶手段と、

上記 IC カード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第 1 の記憶手段か

ら読出し、上記 IC カード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、

この暗号化手段により暗号化した暗号化済みコマンドを上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、

上記 IC カード処理装置が、

上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第 1 の送信手段と、

この第 1 の送信手段に回答して上記キーカードから得られる暗号化済みコマンドを上記 IC カードへ送信する第 3 の送信手段とからなり、

上記 IC カードが、

暗号化キーを記憶している第 2 の記憶手段と、

上記暗号化キーを上記第 2 の記憶手段により読出し、この読出した暗号化キーに基づいて上記 IC カード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、

ことを特徴とする IC カード処理システム。

【請求項 10】 IC カード処理装置と IC カードとキーカードとからなる IC カード処理システムにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第 1 の記憶手段と、

上記 IC カード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第 1 の記憶手段から読出し、上記 IC カード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、

この暗号化手段により暗号化した暗号化済みコマンドを上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、

上記 IC カード処理装置が、

上記 IC カードに対して指定キー番号を送信する第 1 の送信手段と、

上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第 2 の送信手段と、

この第 2 の送信手段に回答して上記キーカードから得られる暗号化済みコマンドを上記 IC カードへ送信する第 3 の送信手段とからなり、

上記 IC カードが、

指定キー番号に対応する種々の暗号化キーを記憶している第 2 の記憶手段と、

上記 IC カード処理装置からの指定キー番号に対応する

暗号化キーを上記第2の記憶手段により読出し、この読出した暗号化キーに基づいて上記ICカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするICカード処理システム。

【請求項11】 ICカードの発行を指示するICカード処理装置と、このICカード処理装置による指示とキーカードからのデータに基づいてICカードを発行するリーダライタとからなるICカード処理システムにおいて、

上記ICカード処理装置が、
ICカードの発行指示を上記リーダライタへ送信する第1の送信手段からなり、
上記リーダライタが、
ICカードへ送信するコマンド電文を生成する生成手段と、

上記ICカード処理装置からのICカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、

この暗号化手段により暗号化されたコマンド電文と上記暗号化キーを上記ICカードへ送信する第2の送信手段とからなり、

上記キーカードが、
暗号化キーを記憶する記憶手段と、
上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第3の送信手段とからなり、
上記ICカードが、

上記リーダライタからの暗号化キーに基づいて、上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするICカード処理システム。

【請求項12】 ICカードの発行を指示するICカード処理装置と、このICカード処理装置による指示とキーカードからのデータに基づいてICカードを発行するリーダライタとからなるICカード処理システムにおいて、

上記ICカード処理装置が、
ICカードの発行指示を上記リーダライタへ送信する第1の送信手段からなり、
上記リーダライタが、

ICカードへ送信するコマンド電文を生成する生成手段と、
上記ICカード処理装置からのICカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成さ

れたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ICカードへ送信する第2の送信手段とからなり、
上記キーカードが、

暗号化キーを記憶する記憶手段と、
上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第3の送信手段とからなり、
上記ICカードが、
上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、

この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするICカード処理システム。

【請求項13】 ICカード処理装置とICカードとからなるICカード処理方法において、
上記ICカード処理装置が、
ICカードに対してカード固有番号の出力要求を上記ICカードへ送信し、

この送信に応答して得られるICカードのカード固有番号を暗号キーとしてコマンド電文を暗号化し、
この暗号化されたコマンド電文を上記ICカードへ送信し、
上記ICカードが、

カード固有番号を記憶している記憶手段と、
上記ICカード処理装置からのカード固有番号の出力要求に応答してあらかじめ記憶されているカード固有番号を上記ICカード処理装置へ送信し、
この送信に応答して得られる暗号化されたコマンド電文を上記カード固有番号を復号キーとして復号化し、

この復号化されたコマンド電文に基づいた処理を行う、
ことを特徴とするICカード処理方法。

【請求項14】 カード固有情報を記憶している記憶手段と、
カード発行装置から暗号化されて送信されるファイル創生コマンドを前記憶手段に記憶しているカード固有情報を復号キーとして復号する復号化手段と、
この復号化手段により復号化されたファイル創生コマンドによりファイルの創生を行なうファイル創生手段と、
このファイル創生手段によるファイル創生が完了した場合上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするICカード。

【請求項15】 請求項14のICカードにおいて、
上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、
ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするICカード。

【請求項16】 請求項14のICカードにおいて、
上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、
ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするICカード。

【請求項17】 請求項14のICカードにおいて、
上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、
ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするICカード。

【請求項18】 請求項14のICカードにおいて、
上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、
ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするICカード。

【請求項19】 請求項14のICカードにおいて、
上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、
ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするICカード。

上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とする IC カード。

【請求項 17】 請求項 14 の IC カードにおいて、上記カード発行装置からの指示に基づき、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とする IC カード 10

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、IC カードの発行時のコマンド等が隠蔽される IC カード処理装置と IC カードと IC カード処理システムと IC カード処理方法に関する。

【0002】

【従来の技術】IC カードは、各運用アプリケーションに従って適宜アプリケーションファイルを IC のメモリ 20 内に生成し、各種キー情報等をそのファイルに対して設定して使用する。ここでは、このアプリケーションごとに共通のファイル生成・キー設定等を「一次発行」と呼び、この一次発行で生成されたファイルにカード個別のデータを設定する作業を「二次発行」と呼ぶ。

【0003】さて、この一次発行は、一般的にカードが理解できる「発行コマンド」を使用する。すなわち、アプリケーションから要求される種々の形のファイルの生成や、そのファイルに設定されるキーデータ等をカード (の OS) に対してコマンドの形で示し、カード (の OS) がこれを解釈して内部メモリ上にファイルを生成する。…(1)

また、IC カードに対して PC (パソコン) 等の機器がデータを送信する場合、PC 等の機器とカードとの間には、カードを保持してカードに対して電源供給や活性化制御等を行なうリーダライタと呼ばれる機器が介在する必要がある。このリーダライタは多くの場合 PC 等と RS-232C や SCSI といった通信インタフェースで通信線を介して PC 等の機器と接続される。…(2)

さらに、この発行コマンドは、PC 等の機器内のプログラムの一部としてその機器内に格納されており、プログラム動作の一つとしてその機器からカードに向けて送出されることになる。…(3)

IC カード内のファイルが(1)の様に生成されるということは、未発行のカードと発行コマンドに関する情報が手に入れば、いかなるカードも作成出来ることになる。

【0004】しかしながら、従来よりこの発行コマンドはカードに対してそのパラメータも含めて裸の状態で作成されているため、カードへのコマンド電文をカード表面の接点やリーダライタの通信線の伝送データをモニタす 50

ること、あるいは PC 等の発行コマンドを送出する機器のプログラムを解析することによって、発行コマンド自体だけでなく、各アプリケーションでどのようなファイルが生成され、どのようなキーやパラメータが設定されるのかを解析することができる状態である。

【0005】現在、発行作業は発行センタといった部外者の立ち入らない、すなわち伝送データのモニタや、機器側プログラムの解析が実行できない環境でのみ行なうことでこのような問題に対抗して来たが、一アプリケーションで複数の異なるファイル構成のカードを使用したり、カードの発注処理・在庫管理の効率化等の要求から、近年、未発行のカードを出先機関や接客窓口に置き、その場で一次発行から実施する運用の要求があり、このような場合、前記のカードセンタでの運用の様に(1)～(3)が実行出来ないように管理することは非常に困難になる。

【0006】

【発明が解決しようとする課題】この発明は、発行対象カードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関する IC カードのセキュリティを向上させることができることを目的とする。

【0007】さらに、この発明は、コマンド電文の暗号化に関する端末機側の処理に使用するデータ類を発行機システムには一般的なキーカードに格納することで、そのセキュリティをより向上させることができることを目的とする。

【0008】また、端末機側での暗・復号処理自体をキーカード内で実施することで、そのセキュリティを更に向上させることができることを目的とする。

【0009】また、このようなキーカードを、キーカードと発行対象のカードの両者を同一筐体内に保持する様な形式のリーダライタで扱う場合、キーカードから出力されるデータをリーダライタ内でクローズして使用することで、そのセキュリティは更に向上することを目的とする。

【0010】

【課題を解決するための手段】この発明の IC カード処理装置は、IC カードへ送信するコマンド電文を生成する生成手段と、IC カードに対してカード固有番号の出力要求を上記 IC カードへ送信する第 1 の送信手段と、この第 1 の送信手段に回答して得られる IC カードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記 IC カードへ送信する第 2 の送信手段と、この第 2 の送信手段に回答して得られる処理結果に応じて処理を終了する終了手段とからなる。

【0011】この発明のICカードは、カード固有番号を記憶している記憶手段と、外部装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記外部装置へ送信する第1の送信手段と、この第1の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段と、この処理手段による処理結果を上記外部装置へ送信する第2の送信手段とからなる。

【0012】この発明のICカード処理システムは、ICカード処理装置とICカードとからなるものにおいて、上記ICカード処理装置が、ICカードへ送信するコマンド電文を生成する生成手段と、ICカードに対してカード固有番号の出力要求を上記ICカードへ送信する第1の送信手段と、この第1の送信手段に応答して得られるICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ICカードへ送信する第2の送信手段とからなり、上記ICカードが、カード固有番号を記憶している記憶手段と、上記ICカード処理装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記ICカード処理装置へ送信する第3の送信手段と、この第3の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0013】この発明のICカード処理システムは、ICカード処理装置とICカードとからなるものにおいて、上記ICカード処理装置が、ICカードへ送信するコマンド電文を生成する生成手段と、ICカードに対してカード固有番号の出力要求を上記ICカードへ送信する第1の送信手段と、この第1の送信手段に応答して得られるICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ICカードへ送信する第2の送信手段と、この第2の送信手段に応答して得られる処理結果が供給された際に、上記生成手段により生成されたコマンド電文の送信を行うか終了するかを判断する判断手段と、この判断手段によりコマンド電文の送信を判断した際に、上記ICカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を上記暗号化手段により暗号化し、上記第2の送信手段により暗号化されたコマンド電文を上記ICカードへ送信する第1の処理手段とからなり、上記ICカードが、カード固有番号を記憶している記憶手段と、上記ICカード処理装置からのカード固有番号の出力要求に応答して上記記

憶手段から読出したカード固有番号を上記ICカード処理装置へ送信する第3の送信手段と、この第3の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う第2の処理手段と、この第2の処理手段による処理結果を上記ICカード処理装置へ送信する第4の送信手段とからなる。

【0014】この発明のICカード処理システムは、ICカード処理装置とICカードとからなるものにおいて、上記ICカード処理装置が、ICカードへ送信するコマンド電文を生成する第1の生成手段と、ICカードに対して乱数の出力要求を上記ICカードへ送信する第1の送信手段と、この第1の送信手段に応答して得られるICカードからの乱数を暗号キーとして上記第1の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ICカードへ送信する第2の送信手段とからなり、上記ICカードが、カード固有番号を記憶している記憶手段と、この記憶手段から読出したカード固有番号に基づく乱数を生成する第2の生成手段と、上記ICカード処理装置からの乱数の出力要求に応答して上記第2の生成手段により生成される乱数を上記ICカード処理装置へ送信する第3の送信手段と、この第3の送信手段に応答して得られる暗号化されたコマンド電文を上記第2の生成手段により生成される乱数を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0015】この発明のICカード処理システムは、ICカード処理装置とICカードとからなるものにおいて、上記ICカード処理装置が、前回の乱数を記憶する記憶手段と、この記憶手段により読出した前回の乱数に基づく乱数を生成する第1の生成手段と、ICカードへ送信するコマンド電文を生成する第2の生成手段と、上記第1の生成手段により生成される乱数を上記ICカードへ送信する第1の送信手段と、この第1の送信手段に応答して得られるICカードからの処理準備開始応答が供給された際に、上記第1の生成手段により生成される乱数を暗号キーとして上記第2の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ICカードへ送信する第2の送信手段と、この第2の送信手段に応答して得られるICカードからの応答が供給された際に、上記第1の生成手段により生成される乱数を暗号キーとして上記第2の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記ICカードへ上記第2の送信手段で送信する第1の処理手段とからなり、上記ICカードが、上記ICカード処理装置からの乱数に基づいて、処理準

備開始応答を上記 IC カード処理装置へ送信する上記第 3 の送信手段と、上記 IC カード処理装置からの乱数に基づいて、上記第 3 の送信手段に回答して得られる暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う第 2 の処理手段と、この第 2 の処理手段による処理結果を上記 IC カード処理装置へ送信する第 4 の送信手段と、この第 4 の送信手段に回答して得られる暗号化されたコマンド電文を、上記復号化手段で上記 IC カード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第 2 の処理手段で行う第 3 の処理手段とからなる。

【0016】この発明の IC カード処理システムは、IC カード処理装置と IC カードとからなるものにおいて、上記キーカードが、上記 IC カード処理装置から与えられる前回処理に使用された乱数を記憶する第 1 の記憶手段、認証データを記憶する第 2 の記憶手段と、上記 IC カード処理装置からの認証データと上記第 2 の記憶手段に記憶されている認証データとが一致した際に、上記第 1 の記憶手段に記憶されている前回の乱数を上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、上記 IC カード処理装置が、上記キーカードへ認証データを送信する第 2 の送信手段と、この第 2 の送信手段に回答して上記キーカードから得られる前回の乱数に基づく乱数を生成する第 1 の生成手段と、この第 1 の生成手段で生成された乱数を上記キーカードへ送信する第 3 の送信手段と、IC カードへ送信するコマンド電文を生成する第 2 の生成手段と、上記第 1 の生成手段により生成される乱数を上記 IC カードへ送信する第 4 の送信手段と、この第 4 の送信手段に回答して得られる IC カードからの処理準備開始応答が供給された際に、上記第 1 の生成手段により生成される乱数を暗号キーとして上記第 2 の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記 IC カードへ送信する第 5 の送信手段と、この第 5 の送信手段に回答して得られる IC カードからの応答が供給された際に、上記第 1 の生成手段により生成される乱数を暗号キーとして上記第 2 の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記 IC カードへ上記第 5 の送信手段で送信する第 1 の処理手段とからなり、上記 IC カードが、上記 IC カード処理装置からの乱数に基づいて、処理準備開始応答を上記 IC カード処理装置へ送信する上記第 6 の送信手段と、上記 IC カード処理装置からの乱数に基づいて、上記第 6 の送信手段に回答して得られる暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う第 2 の処理手段と、この第 2 の処理手段による処理結果を上記 IC カード処理装置へ送信する第 7 の送信手段と、この第 7 の

送信手段に回答して得られる暗号化されたコマンド電文を、上記復号化手段で上記 IC カード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第 2 の処理手段で行う第 3 の処理手段とからなる。

【0017】この発明の IC カード処理システムは、IC カード処理装置と IC カードとからなるものにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドを記憶する第 1 の記憶手段と、上記 IC カード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第 1 の記憶手段から読出し、この読出したコマンドを上記 IC カード処理装置からの暗号キーに基づいて暗号化する暗号化手段と、この暗号化手段により暗号化した暗号化済みコマンドを上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、上記 IC カード処理装置が、上記 IC カードに対してカード固有番号の出力要求を送信する第 1 の送信手段と、上記キーカードへ指定コマンド番号と実行パラメータと上記第 1 の送信手段に回答して得られる IC カードのカード固有番号としての暗号キーを送信する第 2 の送信手段と、この第 2 の送信手段に回答して上記キーカードから得られる暗号化済みコマンドを上記 IC カードへ送信する第 3 の送信手段とからなり、上記 IC カードが、カード固有番号を記憶している第 2 の記憶手段と、上記 IC カード処理装置からのカード固有番号の出力要求に回答して上記第 2 の記憶手段から読出したカード固有番号を上記 IC カード処理装置へ送信する第 3 の送信手段と、この第 3 の送信手段に回答して得られる暗号化されたコマンド電文を上記第 2 の記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0018】この発明の IC カード処理システムは、IC カード処理装置と IC カードとからなるものにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第 1 の記憶手段と、上記 IC カード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第 1 の記憶手段から読出し、上記 IC カード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、この暗号化手段により暗号化した暗号化済みコマンドを上記 IC カード処理装置へ送信する第 1 の送信手段とからなり、上記 IC カード処理装置が、上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第 1 の送信手段と、この第 1 の送信手段に回答して上記キーカードから得られる暗号化済みコマンドを上記 IC カードへ送信す

る第3の送信手段とからなり、上記ICカードが、暗号化キーを記憶している第2の記憶手段と、上記暗号化キーを上記第2の記憶手段により読出し、この読出した暗号化キーに基づいて上記ICカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0019】この発明のICカード処理システムは、ICカード処理装置とICカードとからなるものにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第1の記憶手段と、上記ICカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第1の記憶手段から読出し、上記ICカード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、この暗号化手段により暗号化した暗号化済みコマンドを上記ICカード処理装置へ送信する第1の送信手段とからなり、上記ICカード処理装置が、上記ICカードに対して指定キー番号を送信する第1の送信手段と、上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第2の送信手段と、この第2の送信手段に回答して上記キーカードから得られる暗号化済みコマンドを上記ICカードへ送信する第3の送信手段とからなり、上記ICカードが、指定キー番号に対応する種々の暗号化キーを記憶している第2の記憶手段と、上記ICカード処理装置からの指定キー番号に対応する暗号化キーを上記第2の記憶手段により読出し、この読出した暗号化キーに基づいて上記ICカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0020】この発明のICカード処理システムは、ICカードの発行を指示するICカード処理装置と、このICカード処理装置による指示とキーカードからのデータに基づいてICカードを発行するリーダライタとからなるものにおいて、上記ICカード処理装置が、ICカードの発行指示を上記リーダライタへ送信する第1の送信手段とからなり、上記リーダライタが、ICカードへ送信するコマンド電文を生成する生成手段と、上記ICカード処理装置からのICカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文と上記暗号化キーを上記ICカードへ送信する第2の送信手段とからなり、上記キーカードが、暗号化キーを記憶する記憶手段と、上記リーダライタからの指示に基づいて暗号化キーを上記リー

ダライタへ送信する第3の送信手段とからなり、上記ICカードが、上記リーダライタからの暗号化キーに基づいて、上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0021】この発明のICカード処理システムは、ICカードの発行を指示するICカード処理装置と、このICカード処理装置による指示とキーカードからのデータに基づいてICカードを発行するリーダライタとからなるものにおいて、上記ICカード処理装置が、ICカードの発行指示を上記リーダライタへ送信する第1の送信手段とからなり、上記リーダライタが、ICカードへ送信するコマンド電文を生成する生成手段と、上記ICカード処理装置からのICカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ICカードへ送信する第2の送信手段とからなり、上記キーカードが、暗号化キーを記憶する記憶手段と、上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第3の送信手段とからなり、上記ICカードが、上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【0022】この発明のICカードは、カード固有情報を記憶している記憶手段と、カード発行装置から暗号化されて送信されるファイル創生コマンドを前記記憶手段に記憶しているカード固有情報を復号キーとして復号する復号化手段と、この復号化手段により復号化されたファイル創生コマンドによりファイルの創生を行なうファイル創生手段と、このファイル創生手段によるファイル創生が完了した場合上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしている。

【0023】

【発明の実施の形態】以下、図面を参照してこの発明のICカード処理システムとしてのICカード発行システムを説明する。

【0024】このICカード発行システムは、出先機関や接客窓口に設置した不特定多数の人間が触れることができる環境で運用される機器により構成され、伝送データのモニタや、機器側プログラムの解析を回避することがなされている。

【0025】図1は、この発明のICカード発行システムのブロックを示している。

【0026】この実施形態では、コマンド電文自体を、受信したカードだけでは解釈する事ができない形式に暗

号化してカードに対して送信することにより、カードへのコマンド電文をモニタしても、発行コマンドに関する情報の漏洩が防止でき、発行処理に関するICカードのセキュリティを向上できる。未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止できる。

【0027】このICカード発行システムは、図1に示すように、パソコン(PC)1とこのPC1と通信ライン2を介して接続されているリーダライタ3とからなる。このリーダライタ3には、図示しないコネクタ等で接続される発行対象カードとしてのICカード4が装着されるようになっている。

【0028】PC1は、PC1の全体を制御する制御部5、制御用のプログラムが記憶されていたり種々のデータが記憶されるメモリ6、操作指示を行うキーボード等の操作部7、操作案内等が表示される表示部8、リーダライタ3とのデータのやり取りを行うインターフェース9により構成されている。

【0029】上記制御部5としては、ICカード4から供給される製造番号(カード固有情報)を暗号キーとしてコマンド電文の暗号化を行う暗号化機能を有している。メモリ6から読取った各カードに対する共通の暗号キーとしてコマンド電文の暗号化を行う暗号化機能(第1の実施形態)、ICカード4から供給される製造番号を暗号キーとしてコマンド電文の暗号化を行う暗号化機能(第2の実施形態)、ICカード4から供給される乱数を暗号キーの種としてコマンド電文の暗号化を行う暗号化機能(第3の実施形態)を有し、上記暗号化プログラム(制御部処理プログラム)はROM15に格納されている。また、上記CPU14は、生成された乱数を格納する乱数バッファをメモリ6に用意している(第3、第4の実施形態)。

【0030】リーダライタ3は、リーダライタ3の全体を制御するCPU10、制御用のプログラムが記憶されていたり種々のデータが記憶されるメモリ11、PC1とのデータのやり取りを行うインターフェース12、ICカード4とのデータのやり取りを行うインターフェース13により構成されている。また、リーダライタ3には、ICカード4の挿入検知を行う検知器(図示しない)を有し、この検知結果をPC1へ出力するようになっている。また、リーダライタ3は、ICカード4の挿入検知時にICカード4の内容を読取り、アプリケーション等が未記録の発行用のカードか否かを示すデータをPC1へ出力するようにしても良い。

【0031】ICカード4は、図2に示すように、ICカード4の全体を制御するCPU14、カード内部動作の制御用のプログラムが記憶されているROM15、外部(リーダライタ3)と交換する電文の送受信バッファとCPU14の処理中のデータの一時格納バッファとして利用されるRAM16、アプリケーション運用でその

値内容をリードライトして使用される運用データが格納され、電文隠蔽用キーデータとしてのカード固有の製造番号等が格納されるEEPROM17、リーダライタ3とのデータのやり取りを行うインターフェース18により構成されている。

【0032】上記CPU14としては、EEPROM17から読取った各カードで共通の復号キーとして暗号化済みのコマンド電文の復号化を行う復号化機能(第1の実施形態)、EEPROM17から読取った製造番号を復号キーとして暗号化済みのコマンド電文の復号化を行う復号化機能(第2の実施形態)、EEPROM17から読取った製造番号に基づいて乱数生成ロジックにより生成される乱数を復号キーの種として暗号化済みのコマンド電文の復号化を行う復号化機能(第3の実施形態)を有し、上記復号化プログラム(CPU処理プログラム)はROM15に格納されている。また、上記EEPROM17には、乱数を格納する乱数バッファが設けられている(第3、第4の実施形態)。

【0033】PC1は、図3に示すように、主制御プログラム、発行コマンドテンプレート、発行情報ファイル等の機能を有している。発行コマンドテンプレートは、図4に示すような、各コマンド種別ごとにカードが解釈できるコマンド電文フォーマットの平文形式でのテンプレートである。主制御プログラムは、外部から記憶媒体や通信等でPC1に一对して与えられる発行情報ファイルの内容に従ってコマンドテンプレートから適用されるものを選択し、発行情報ファイル内のパラメータをテンプレートにセットして平文のコマンド電文を完成させた上でそれを暗号化してから発行対象カード(ICカード4)が装着されているリーダライタ3を経由して発行対象カード(ICカード4)に対して送信するようになっている。

【0034】図4に示す、コマンドテンプレートとしては、フォルダ/ファイル生成コマンドテンプレートとキー設定コマンドテンプレートとからなる。フォルダ/ファイル生成コマンドテンプレートは、フォルダ/ファイル生成コマンドコード、フォルダ/ファイル指定(実行パラメータ)、フォルダ/ファイル管理情報(処理用データ)により構成され、キー設定コマンドテンプレートは、キー設定コマンドコード、キーファイル(ID)指定(実行パラメータ)、キーデータ長(処理用データ)、実キーデータ部(処理用データ)により構成されている。

【0035】図5は、ICカード4に対するコマンド電文の一般形の例を示す。このコマンド電文は、先頭符号21、送信電文長22、コマンドコード23、実行パラメータ24、処理用データ25、末尾符号26により構成されている。先頭符号21、送信電文長22、末尾符号26は、実際のコマンドを示すブロック(コマンドコード23、実行パラメータ24、処理用データ25;コ

10

20

30

40

50

マンド処理内容表示部分)を運ぶために標準規格化されているプロトコルで規定される部分(トレーラ)であり、暗号化の対象とはならない。

【0036】なお、一般的にはそのコマンド電文が暗号化されたものか否かを示す必要があり、その様な情報は先頭符号21を2種規定し平文と暗号文とで使い分ける方法が用いられる。または、受信されたコマンド電文をとりあえず平文としてとらえて、解釈不能の時にだけ暗号文としての処理を試行するという方法を用いても良い。但し、その際には暗号化の際に暗号化後の電文が平文のコマンド電文と全く同一とならないようにする。

【0037】上記トレーラで運ばれるブロックの内容のうち、コマンドコード23はICカード4に対して要求する処理の種別(発行コマンドの例では「ファイルの創成」等)を表し、実行パラメータ24はコマンドコードで示された処理種別の中での処理内容の詳細パラメータ(発行コマンドの「ファイル創成」の例では「創成するファイルの種類」等)を表し、処理用データ25はコマンドコードで示された処理種別の中での処理パラメータだけでは表しきれない付帯情報(発行コマンドの「ファイル創成」の例では「創成するファイルの名前やサイズ」等)を表す。これらが暗号化対象となり、暗号化済みのコマンド電文は図6に示すように、先頭符号21、送信電文長22、コマンドコード23と実行パラメータ24と処理用データ25とのブロックを暗号化したデータ27、末尾符号26により構成される。

【0038】このとき、暗号化前後で送信電文長22すなわちコマンド処理を示すブロックの暗号化前後の長さは、同じあるいは変化するようになっている。

【0039】上記ICカード1のEEPROM17内に格納するデータは、図7に示す様なPC1と類似のフォルダ、ファイルのツリー構造イメージで管理される。

【0040】図7は、3アプリケーションすなわち3種のサービスが相乗りしたカードを想定している。

【0041】ここで言うアプリケーションとは、たとえば、買い物金額に応じてポイントが与えられる百貨店の会員システムに、座席予約情報やマイレッジといったデータを格納し利用する旅客航空会社の会員システムと、トレーニング履歴や健康診断情報を蓄積していき健康増進に役立てるフィットネスクラブの会員システムが相乗りしたイメージととらえる。

【0042】すると、アプリケーションフォルダ1が百貨店用、アプリケーションフォルダ2が航空会社用、アプリケーションフォルダ3がフィットネスクラブ用である。

【0043】航空会社用のフォルダ2の配下にある各データファイルは航空会社が管理する会員情報と座席予約情報を格納し、アプリケーションフォルダ2'は特にマイレッジ関係のデータを格納するために利用されるものととらえることができる。

【0044】次に、これらのフォルダ、ファイルの管理情報の例を図8、図9、図10に示す。

【0045】まず、図8はアプリケーションフォルダの管理情報の例である。このアプリケーションフォルダ管理情報は、フォルダ名称、フォルダサイズ、上位フォルダ、参照アクセス権、および変更アクセス権により構成されている。

【0046】フォルダ名称としては、たとえば百貨店の会員システム用フォルダなら百貨店名としたり、何らかの任意の文字列を当てることができる。フォルダを識別するためのものなので1枚のカード内のフォルダの名称は全て異ならなければならないが、全てのカードについて各アプリケーション用のフォルダ名称は同一となっている。

【0047】フォルダサイズは、配下に生成される全ファイルを格納するのに足るメモリ容量を示す。ICカード4のEEPROM17内へのファイル生成の手順としては、まず各アプリケーション用フォルダを生成して次のステップとして各フォルダ配下にフォルダないしはファイルを生成していくことになる。このため、各アプリケーション用フォルダが必要とするメモリ容量をEEPROM17上に確保するのにこのサイズ情報が必要となる。

【0048】上位フォルダは、たとえば図7のアプリケーション2フォルダ配下にアプリケーション2'フォルダを生成する様な場合、アプリケーション2'フォルダ生成タイミングでアプリケーション2フォルダを上位フォルダとして指定する。

【0049】アプリケーション1~3の各フォルダ生成時には、マスタフォルダを上位フォルダとして指定する。

【0050】参照アクセス権および変更アクセス権は、そのフォルダ内にデータファイルやキーファイルを参照あるいは、生成、削除等するのに先だって照合済みあるいは認証済みの状態にされていなければならないキーがどれであるかを示す。

【0051】マスタフォルダ配下のアプリケーション用フォルダでは、マスタフォルダ直下のマスタファイル用キーフォルダのいずれかを、また、アプリケーション2'フォルダにおいてはアプリケーション2フォルダ直下のアプリケーション2用キーフォルダのいずれかを指定することになる。

【0052】たとえば、マスタフォルダ直下のギーデータファイルに対する各アクセス権は、EEPROM17の特定アドレスにデータを直接書き込む様な方法により製造段階に与えるキーにより管理される。

【0053】次に、図9はキーファイルの管理情報の例である。キーファイル管理情報は、ファイルID、キーデータ長、キー種別、参照アクセス権、および変更アクセス権により構成されている。

10

20

30

40

50

【0054】あるキーを特定してアクセスするため各キーにはファイルIDが付与される。但し、異なるアプリケーションフォルダ内のキーについては、アプリケーションフォルダを指定することで区別ができるため同一のキーIDを付与することも許容される。

【0055】また、ICカード4ではキーデータは可変長であり、キーデータ長でそのキーデータの長さを示す。

【0056】キー種別とは、単純に外部から与えられたキー値と比較される照合用のキーデータなのか、外部から与えられた数値と比較するために先に出力している乱数をカード内部で暗号化する際に使用するためのキーデータとして使用する認証用のキーデータなのかを示す。

【0057】参照アクセス権は、そのキーの照合処理あるいは認証処理を実行するために必須の他のキーの照合済みあるいは認証済み状態を示す。

【0058】変更アクセス権は、先に設定されているキーデータ自体を変更する際に必須の他のキーの照合済みあるいは認証済み状態を示す。

【0059】次に、図10はデータファイルの管理情報の例である。データファイル管理情報は、ファイルID、ファイルサイズ、ファイル種別、参照アクセス権、および変更アクセス権により構成されている。

【0060】ファイルIDについてはキーデータファイルと同一の考え方で付与される。またアプリケーション運用に使用されるデータは用途ごとにデータの長さがあらかじめ想定されているため、それに合わせてファイルサイズを示す。

【0061】ファイル種別とは、ファイルデータの管理方法として、単純なデータの羅列としてメモリ空間を解放するだけのファイルなのか、データをレコードイメージで区切ってカード内でアクセス管理するファイルなのかを示す。

【0062】参照アクセス権は、そのデータの参照すなわち読み出しを実行するために必須の他のキーの照合済みあるいは認証済み状態を示す。

【0063】変更アクセス権は、変更すなわち書き換えを実行する際に必須の他のキーの照合済みあるいは認証済み状態を示す。

【0064】上記各管理情報をICカード4に対してコマンド電文で送り込むことがICカード4の一次発行処理となる。

【0065】すなわち、図4の様に図5のコマンド電文の処理用データとして上記管理情報を与え、コマンドコードと実行パラメータを図4の様に設定してICカード4に対して送信することで、ICカード4は管理情報に従ってEEPROM17内にメモリ空間を確保し各ファイルを設定していく。

【0066】次に、通信ライン2におけるコマンド電文を暗号化する方法について説明する。

【0067】まず、第1の実施形態として、最も簡単な方法について説明する。

【0068】すなわち、図1に示す構成において、カード製造時に全てのICカード4に同一の復号ロジックと復号鍵を持たせ、ICカード4に対するコマンド電文を送信するPC1側にも、これらに対応した暗号ロジックと暗号キーを持たせる。

【0069】すなわち、一次発行処理では全てのICカード4に対してシステムごと共通のファイルを作成するため、全てのICカード4に同一の復号ロジック（具体的にはプログラム）と鍵（復号キー）を使用する。この場合、暗号化後のコマンド電文は全てのICカード4に対して同一とはなるが、少なくとも図5の様な裸の状態の「コマンド」を隠蔽することはできる。

【0070】次に、第2の実施形態として、暗号化したコマンド電文をICカード4ごとに個別にする場合について、図11に示すフローチャートと図12に示す状態遷移図を用いて説明する。

【0071】この場合、ICカード4の個別データとして、製造時にICカード4のEEPROM17に格納される製造番号を利用する。

【0072】すなわち、一次発行開始時に、PC1は、ICカード4のEEPROM17から製造番号を読み出し、この値をそのまま、あるいは加工を施した上で暗号化のキーに使用して暗号化したコマンド電文をICカード4に送る。これにより、ICカード4の内部では同様に製造番号を使用して受信したコマンド電文を解釈する。

【0073】まず、PC1の表示部8の画面上の発行機アイコンをクリックする(ST1)。すると、制御部5はICカードの発行を判断し、表示部8により発行用のICカード4のリーダライタ3への挿入要求が表示される(ST2)。

【0074】この表示に基づいて、発行用のICカード4がリーダライタ3に挿入される(ST3)。

【0075】この挿入の検知信号（リーダライタ3からPC1の制御部5へ出力）に基づいて、制御部5は表示部8により発行機プログラムメインメニューを表示し

(ST4)、発行機アプリケーションを起動する(ST5)。このメニュー表示により、操作部7により発行カード種別を選択し(ST6)、一次発行処理を選択する(ST7)。これにより、制御部5は発行情報ファイルの1ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、1ステップ分のコマンド電文を生成し、メモリ6に記憶する(ST8)。

【0076】この状態において、PC1の制御部5からICカード4のCPU14へ製造番号送出要求が出力される(ST9)。ICカード4のCPU14はEEPROM17に記憶されている製造番号を読み出し、PC1の

制御部5に出力される(ST10)。これにより、PC1の制御部5は供給される製造番号をキーとしてメモリ6に記憶するとともに、その製造番号をキーとして上記メモリ6に記憶されている1ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力される(ST11)。ICカード4のCPU14はEEPROM17に記憶されている製造番号をキーとして読出し、この読出した製造番号を復号キーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST12)、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する(ST13)。このコマンドによる処理の結果をPC1の制御部5に出力される(ST14)。

【0077】これにより、PC1の制御部5は処理結果としてのICカード4からのレスポンス電文を受信し(ST15)、そのレスポンス内容を確認する(ST16)。このレスポンス内容の確認後、次の発行情報ファイルがある場合(ST17)、PC1の制御部5は発行情報ファイルの次の1ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、1ステップ分のコマンド電文を生成し、メモリ6に記憶する(ST18)。

【0078】これにより、PC1の制御部5は上記メモリ6に記憶されている次の1ステップ分の発行情報ファイルとしてのコマンド電文を上記メモリ6に記憶されている製造番号をキーとして暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力される(ST11)。ICカード4のCPU14はEEPROM17に記憶されている製造番号をキーとして読出し、この読出した製造番号をキーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST12)、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する(ST13)。このコマンドによる処理の結果がPC1の制御部5に出力される(ST14)。

【0079】これにより、PC1の制御部5は処理結果としてのICカード4からのレスポンス電文を受信し(ST15)、そのレスポンス内容を確認する(ST16)。

【0080】以後、発行情報ファイルのステップ内容がなくなるまで、ステップ18、11から16が繰り返され、上記ステップ17で次の発行情報ファイルの無しが判断された際に処理を終了する。

【0081】この例ではICカード4の個別データの分かりやすい代表例として製造番号を使用しているが、コマンド電文の隠蔽を目的とする場合、必ずしもICカード4の製造番号である必要はなく、ICカード4の個別の完全ユニーク性についても必須の条件ではない。

【0082】次に、第3の実施形態として、暗号化のキ

ーをコマンド電文生成の都度、異ならせる場合について説明する。

【0083】基本的に一枚のICカード4に対する一次発行処理は、ICカード4のライフサイクルを通して一回だけのものだが、発行コマンドの機能、形式によっては、ICカード4に対して類似のコマンドを多数回送出するケースが考えられる。

【0084】たとえば、1ファイルの創成について、1回のコマンド送信が必要な場合、創成するファイルの形式に関する情報だけが異なる同一のコマンドを、創成するファイルの数だけ送出するため暗号化された電文の解析の機会が増えることになる。

【0085】また、キーとして使われる製造番号は一次発行処理の始めの段階で生の値として読み出されるため、複数のICカード4を使用して多数の解析用データを集めることも可能である。

【0086】このとき、暗号化のキーに製造番号の様な一律の値を使用することは解析の容易性を増すので、解析をより困難にするため、ICカード4内で暗号化に使用する値を都度異ならせる。この場合、各ICカード4のユニーク性を確保するためICカード4の個別の値として製造番号を利用するが、そのままの値ではなく、それを種にして乱数を乱数生成ロジックを利用して生成する。この生成した乱数を次の種にして新たな乱数を乱数生成ロジックを利用して生成する。

【0087】このように、直前に生成・出力した乱数を次の乱数の種にすることで、都度異なる値(キーとして利用する乱数)が生成される。始めの種がICカード4の個別の値(製造番号)なので、生成される乱数は各ICカード4ごとにも異なる。上記第3の実施形態の一例を、図13、図14に示すフローチャートと図15に示す状態遷移図を用いて説明する。

【0088】まず、PC1の表示部8の画面上の発行機アイコンをクリックする(ST21)。すると、制御部5はICカードの発行を判断し、表示部8により発行用のICカード4のリーダライタ3への挿入要求が表示される(ST22)。

【0089】この表示に基づいて、発行用のICカード4がリーダライタ3に挿入される(ST23)。

【0090】この挿入の検知信号(リーダライタ3からPC1の制御部5へ出力)に基づいて、制御部5は表示部8により発行機プログラムメインメニューを表示し

(ST24)、発行機アプリケーションを起動する(ST25)。このメニュー表示により、操作部7により発行カード種別を選択し(ST26)、一次発行処理を選択する(ST27)。これにより、制御部5は発行情報ファイルの1ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、1ステップ分のコマンド電文を生成し、メモリ6に記憶する(ST28)。

【0091】この状態において、PC1の制御部5からICカード4のCPU14へ乱数送出要求が出力される(ST29)。ICカード4のCPU14はEEPROM17に記憶されている製造番号を読み出し、この読み出した製造番号に基づいて乱数生成ロジックにより乱数を生成し、EEPROM17の乱数バッファに記憶し、その乱数をPC1の制御部5に出力する(ST30)。また、ICカード4のCPU14はEEPROM17の乱数バッファの乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する(ST31)。

【0092】また、PC1の制御部5は供給される乱数を暗号キーとして上記メモリ6に記憶されている1ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力される(ST32)。また、PC1の制御部5は供給される乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、メモリ6の乱数バッファに記憶する(ST33)。

【0093】ICカード4のCPU14はEEPROM17の乱数バッファに記憶されている乱数を復号キーとして読み出し、この読み出した乱数を復号キーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST34)、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する(ST35)。このコマンドによる処理の結果をPC1の制御部5に出力される(ST36)。

【0094】これにより、PC1の制御部5は処理結果としてのICカード4からのレスポンス電文を受信し(ST37)、そのレスポンス内容を確認する(ST38)。このレスポンス内容の確認後、次の発行情報ファイルがある場合(ST39)、PC1の制御部5は発行情報ファイルの次の1ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、1ステップ分のコマンド電文を生成し、メモリ6に記憶する(ST40)。

【0095】これにより、PC1の制御部5は上記メモリ6に記憶されている次の1ステップ分の発行情報ファイルとしてのコマンド電文を上記メモリ6の乱数バッファに記憶されている乱数を暗号キーとして暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力される(ST41)。また、PC1の制御部5はメモリ6の乱数バッファに記憶されている乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する(ST42)。

【0096】また、ICカード4のCPU14はEEPROM17の乱数バッファに記憶されている乱数を復号キーとして読み出し、この読み出した乱数を復号キーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST43)、暗号化されているコマンド電文を

解凍し、このコマンドの処理を実行する(ST44)。このコマンドによる処理の結果がPC1の制御部5に出力される(ST45)。また、ICカード4のCPU14はEEPROM17の乱数バッファの乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する(ST46)。

【0097】これにより、PC1の制御部5は処理結果としてのICカード4からのレスポンス電文を受信し(ST47)、そのレスポンス内容を確認し(ST48)、ステップ39に戻る。

【0098】以後、発行情報ファイルのステップ内容がなくなるまで、ステップ39から48が繰り返され、上記ステップ39で次の発行情報ファイルの無しが判断された際に処理を終了する。

【0099】次に、第4の実施形態として、解析をより困難にするためICカード4内で暗号化に使用する値を都度異ならせる別の手段としてICカード4の個別の製造番号を利用するのではなく、外部からの都度異なるキーを用いる場合について説明する。

【0100】すなわち、第3の実施形態で使用しているICカード4の製造番号の代わりに、はじめにPC1側から乱数の種をICカード4に対して与え、以降は製造番号を種とするのと同様に直前に生成した乱数を種にしていく方法である。この場合、PC1側で始めにICカード4に対して与える乱数をICカード4ごとに異ならせることで、上記第3の実施形態のICカード4の製造番号を利用する方法と同様のICカード4の個別性が確保される。PC1からICカード4に与える乱数を都度異ならせる方法としては、都度PC1の乱数生成機能を使用する他、直前の発行処理時にICカード4に対して与えた乱数を格納しておいて、これを種に新たな乱数を生成する手法等が考えられる。

【0101】また、ICカード4側の処理としては、PC1から乱数が与えられない限り一次発行処理が開始できない制御とすることで、不正な発行を阻止する効果がより大きくなる。

【0102】上記第4の実施形態の一例を、図16に示すフローチャートと図17に示す状態遷移図を用いて説明する。ただし、第2の実施形態の図12のフローチャートと同一部分については同一のステップ番号を付与し説明を省略する。

【0103】ステップ8の状態において、PC1の制御部5は、あらかじめ前回の乱数(メモリ6に記憶)に基づいて乱数生成ロジックにより生成され乱数バッファに記憶されている初期乱数をICカード4のCPU14へ出力する(ST9')。この新たな乱数生成時に、前回の乱数が更新される。ICカード4のCPU14はEEPROM17の一時的乱数バッファに供給される乱数を記憶し、処理準備開始応答をPC1の制御部5へ出力する(ST10')。これにより、PC1の制御部5は供

給される処理準備開始応答により乱数バッファに記憶されている乱数をキーとして上記メモリ6に記憶されている1ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力される(ST11')。ICカード4のCPU14はEEPROM17の一時的乱数バッファに記憶されている乱数をキーとして読出し、この読出した乱数を復号キーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST12')、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する(ST13)。このコマンドによる処理の結果をPC1の制御部5に出力される(ST14)。

【0104】これにより、PC1の制御部5は処理結果としてのICカード4からのレスポンス電文を受信し(ST15)、そのレスポンス内容を確認する(ST16)。このレスポンス内容の確認後、次の発行情報ファイルがある場合(ST17)、PC1の制御部5は発行情報ファイルの次の1ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、1ステップ分のコマンド電文を生成し、メモリ6に記憶する(ST18)。

【0105】これにより、PC1の制御部5は上記メモリ6に記憶されている次の1ステップ分の発行情報ファイルとしてのコマンド電文を上記メモリ6の乱数バッファに記憶されている乱数をキーとして暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力される(ST11')。ICカード4のCPU14はEEPROM17の一時的乱数バッファに記憶されている乱数をキーとして読出し、この読出した乱数をキーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST12')、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する(ST13)。このコマンドによる処理の結果がPC1の制御部5に出力される(ST14)。

【0106】これにより、PC1の制御部5は処理結果としてのICカード4からのレスポンス電文を受信し(ST15)、そのレスポンス内容を確認する(ST16)。

【0107】以後、発行情報ファイルのステップ内容がなくなるまで、ステップ18、11'、12'、13から16が繰り返され、上記ステップ17で次の発行情報ファイルの無しが判断された際に処理を終了する。

【0108】このようにして、発行処理が終了した際に、制御部5は最終の乱数を前回生成乱数としてメモリ6に記憶するようにしても良い。

【0109】上記第4の実施形態の他例を、図18に示すフローチャートと図19に示す状態遷移図を用いて説明する。ただし、第3の実施形態の図13、図14のフローチャートと同一部分については同一のステップ番号

を付与し説明を省略する。

【0110】ステップ28の状態において、PC1の制御部5はあらかじめ前回の乱数(メモリ6に記憶)に基づいて乱数生成ロジックにより生成される初期乱数をICカード4のCPU14へ出力する(ST29')。この新たな乱数生成時に、前回の乱数が更新される。また、PC1の制御部5は上記初期乱数に基づいて乱数生成ロジックにより生成される乱数をメモリ6の乱数バッファに記憶する(ST30')。ICカード4のCPU14は供給される乱数に基づいて乱数生成ロジックにより生成される乱数をEEPROM17の乱数バッファに記憶し、処理準備開始応答をPC1の制御部5へ出力する(ST31')。これにより、PC1の制御部5は供給される処理準備開始応答によりメモリ6の乱数バッファに記憶されている乱数を暗号キーとして上記メモリ6に記憶されている1ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ICカード4のCPU14へ出力する(ST32')。また、PC1の制御部5はメモリ6の乱数バッファに記憶されている乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する(ST33')。

【0111】ICカード4のCPU14はEEPROM17の乱数バッファに記憶されている乱数を復号キーとして読出し、この読出した乱数を復号キーとしてPC1からの暗号化済みコマンド電文を復号化することにより(ST34')、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する(ST35)。このコマンドによる処理の結果をPC1の制御部5に出力される(ST36)。また、ICカード4のCPU14はEEPROM17の乱数バッファの乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する(ST36')。

【0112】以後、ステップ37以降は、第3の実施形態の場合と同様である。

【0113】上述したようにしてフォルダ、ファイル生成が一旦完了した後は一次発行に使用するコマンドは不要だけでなく、不正な発行処理を防止する意味でも使用できないようにした方が良い。

【0114】上記第1から第4の実施形態では、発行コマンドを暗号化してICカード4に対して与える形式としているため、発行コマンドを使用できなくするための方法として、暗号化されたコマンドを受け付けなくするようにすれば良い。具体的には、発行処理が完了した時点で、マスタフォルダ直下のあるキーをロックあるいは消去するという方法がある。

【0115】すなわち、その対象となるキーは発行処理開始時に照合され、ICカード4内で暗号・復号関連機能が動作する際には必ずこのキーの照合状態をチェックし、照合されていないあるいはそのキー自体存在しない

場合にはプログラム動作をスキップする様にしておくことで、暗号化されたコマンドはいっさい受け付けられなくなる。

【0116】また、発行処理完了後、一般の運用コマンドについても暗号化機能を利用したい場合は、発行コマンドのコマンドコードを排除する方法を用いても良い。

【0117】すなわち、発行コマンドと運用コマンドのコマンドコードを区別しておき（たとえばICカード4内に発行コマンドのコードをテーブル化しておき）受信された暗号化された電文を解釈した結果が発行コマンドの（発行コマンドテーブル内にある）場合、処理不能の応答を返すだけの動作とする。

【0118】さらに、発行処理の最終段階としてある特定名称のファイルを生成することで発行処理の完了を示す方法を用いても良い。

【0119】すなわち、アプリケーション運用に必要な全てのファイル生成が完了した後、そのICカード4のROM15内のプログラムが認識しているある特定名称のファイルをマスタフォルダ直下に一般のファイル生成コマンドで生成する。ICカード4のプログラムはこのファイルが存在する限り、前記の様な方法で発行コマンドを受け付けられない動作を選択することができる。

【0120】以上は、コマンドを隠蔽することで伝送データのモニタによる解析を阻止するための方法として、外部機器として想定したPC1内に乱数生成ロジックやコマンドの暗号ロジックおよびコマンドの暗号キーや次のICカード4の発行に使用する前回生成した乱数などを格納する形となっているが、乱数生成や暗号化のロジックはPC1のプログラムの一部として、またキーや乱数データは一般的PC1のファイルデータとしてそれぞれ格納するイメージとなる。

【0121】これらの情報のうち、乱数生成や暗号ロジックはDES（デス）といったその論理が公開されているものを使用する場合が多く、プログラム自体を隠蔽することにはあまり意味がなく、そこで使用されるキーデータ、すなわちここでは実際の暗号キーと前回生成乱数こそがセキュリティの要となる。

【0122】したがって、これらを一般的PCのファイルとしてPCに格納しておくことは危険であり、更にこのキー情報を暗号化したり、キー情報自体を別の媒体に格納してPC自体には残さないようにした方がより効果的である。

【0123】以下に、ICカードの発行システムにおいて、キーカードを利用した方法について説明する。

【0124】ICカード発行システムにおいて、キーカードは一般的に使用者を制限するために使用される。つまり、発行機を使用する際には、起動時に発行システムのリーダライタに必ず装着しなくてはならないようになっている。このようなキーカードにキーデータを格納・保管し、暗号化等に使用する場合について説明する。

【0125】図20に、暗号化用キーデータも含んだキーカードCの記憶内容のイメージを示す。

【0126】すなわち、キーカードCの内部構成は、図2に示すICカード4の構成と同様に、CPU、ROM、RAM、EEPROM、インターフェースにより構成されている。

【0127】また、キーカードCには、図20に示すように、発行者キーと、所持者キーと、発行機プログラム起動用のデータとしてのキーカード身分証明データ、カード所持者氏名・番号データと、コマンド電文隠蔽用のデータとしてのコマンド隠蔽用キーデータ（前回生成乱数）とが記憶されるようになっている。

【0128】上記発行者キーと所持者キーの両方がともに照合が一致となった際に、すべてのデータが読出せるようになっている。

【0129】上記キーカードCを用いるICカード発行システムの構成は、図21に示すように、パソコン（PC）1とこのPC1と通信ライン2を介して接続されている上記ICカード4の発行用のリーダライタ3と、PC1と通信ライン30を介して接続されているキーカードC用のリーダライタ31とからなる。上記リーダライタ31には、キーカードCの挿入検知用の検知器（図示しない）が設けられている。なお、図1のICカード発行システムと同一部分については同一符号を付し説明を省略する。

【0130】また、キーカードC用のリーダライタ31が通信ライン30によりPC1と接続される場合について説明したが、図22に示すように、PC1のPCカードスロット32に直接、キーカードC用のリーダライタ31が接続（装着）されるようにしても良い。

【0131】上記のような構成において、上記キーカードCを用いたICカードCの発行について、図23に示すフローチャートを参照しつつ説明する。

【0132】まず、PC1の表示部8の画面上の発行機アイコンをクリックする（ST51）。すると、制御部5はICカードの発行を判断し、表示部8によりキーカードCのリーダライタ31への挿入要求が表示される（ST52）。

【0133】この表示に基づいて、キーカードCがリーダライタ31に挿入される（ST53）。

【0134】この挿入の検知信号（リーダライタ31からPC1の制御部5へ出力）に基づいて、制御部5はキーカードCに対して発行機キーとその照合指示とを出力する（ST54）。これにより、キーカードCの制御部は記憶されている発行機キーと供給された発行機キーとが一致するかどうかを判断し、一致していた場合、照合OKをPC1へ出力し、不一致の場合、照合NGをPC1へ出力する。

【0135】上記ステップ54の照合指示に基づき、照合NGが返送された場合、制御部5は起動処理を中断す

る。また、上記ステップ54の照合指示に基づき、照合OKが返送された場合、制御部5は表示部8により所持者キーの入力要求が表示される（ST55）。

【0136】この表示に基づいて、操作部7により所持者キー（使用者がカード所持者本人で発行機使用有資格者であることを示すための暗証番号）が入力される（ST56）。この入力に基づいて、制御部5はキーカードCに対して所持者キーとその照合指示とを出力する（ST57）。これにより、キーカードCの制御部は記憶されている所持者キーと供給された所持者キーとが一致する10
 か否かを判断し、一致していた場合、照合OKとカード所持者氏名・番号をPC1へ出力し、不一致の場合、照合NGをPC1へ出力する。

【0137】上記ステップ57の照合指示に基づき、照合NGが返送された場合、制御部5は起動処理を中断する。また、上記ステップ57の照合指示に基づき、照合OKとカード所持者氏名・番号が返送された場合、制御部5は発行機使用履歴リスト（EEPROM内）に自動記録する（ST58）。また、制御部5はキーカードCに対してキーカード身分証明データ（真偽判定のデータ）の読出しを出力する（ST59）。これにより、キーカードCの制御部は記憶されているキーカード身分証明データを読出しPC1へ出力する。

【0138】これにより、制御部5は供給されるキーカード身分証明データの内容によりキーカードの真偽を判定する（ST60）。

【0139】このキーカード身分証明データは、たとえば、そのシステム名称の文字列、システム名称やカード所持者の氏名をビット変換等により暗号化した文字列、あるいはシステム別に割り付けられたそれ自体には意味30
 を持たない乱数値等、外部には明かされないデータである。

【0140】PC1内の発行機プログラム自体が確認するためのものである。

【0141】また、実際の発行機プログラム起動処理のコードの一部を格納しておき、カードから読み出してPC1のプログラムの該当部にそれを貼り付ける様な仕組みとすれば、正規の値（コード）がキーカードCから取り出されなければ、発行機プログラム自体起動できないようにすることができる。プログラムの一部（コード内容）40
 を取出して空白とする。

【0142】たとえば、図24の（a）は、制御部5のプログラム処理動作を分かれ道ごとに進行方向を示すことで迷路を抜けるあるいは道路案内をするプログラムにみたまてている。実際には分かれ道にさしかかるたびに左側の1から15に示す方向へ順次進んでいくことで出口あるいは目的地へ到達する事ができるが、途中の7から10のステップを、図24の（b）（c）に示すように、キーカードCに移動してしまい、PC1のプログラムファイルに残さない様にする事で、決して出口ある50

いは目的地へは到達できない様になる。

【0143】上記ステップ60の判定結果がNGの場合、制御部5は起動処理を中断する。また、上記ステップ60の判定結果がOKの場合、制御部5はキーカードCに対してコマンド電文隠蔽用のデータとしてのコマンド隠蔽用キーデータ（前回生成乱数）の読出しを出力する（ST61）。これにより、キーカードCの制御部は記憶されているコマンド隠蔽用キーデータを読出しPC1へ出力する。このコマンド隠蔽用キーデータとしての前回生成乱数がPC1に供給され、メモリ6の乱数バッファに記憶されることにより、制御部5は、ICカード4の発行準備が整う（ST61）。

【0144】この準備が整った後、上記前回生成乱数を用いて上述した第4の実施形態を実施することができる。

【0145】すなわち、第4の実施形態では、前回生成乱数がメモリ6に記憶されていたが、上記例ではキーカードCに記憶されており、発行機の確認（発行機キーの照合）、使用者の暗証照合がなされた後に、キーカードCから上記前回生成乱数が読出せるようになっているので、前回生成乱数に対するセキュリティが高いものとなっている。

【0146】また、ICカード4の発行ごとに制御部5により発行処理により得られた最終の乱数がキーカードC内に前回生成乱数として記憶されるようになっている。

【0147】また、上記キーカードCからの真偽判定データの読み出しに続いて、発行コマンドの隠蔽に利用する暗号キーをPC1がキーカードCから読み出す。すると、PC1の発行機プログラムはキーカードCから取り出したキーデータを使用して以降の暗号化、乱数生成の処理を行ない、処理終了と共にキーデータをプログラム上から削除する。処理終了までにキーカードC内の格納キーデータを更新する必要があるため、処理の終了時には再度キーカードCをリーダライタ31に装着しないと発行機プログラムを終了出来ない様にする。

【0148】但し、図21あるいは図22の様なキーカード専用のリーダライタ31が装着された構成の場合、適宜必要なタイミングでキーカードCにデータを移し、PC1内にデータを留めない様にする事で、セキュリティをより向上させることができる。

【0149】上記したキーカードCを用いたコマンド電文を隠蔽する方法は、PC1内に容易にアクセスできる形でセキュリティの要となるデータ（前回生成乱数）を残すことを回避するために、その前回生成乱数をキーカードCに格納するものである。

【0150】しかし、既存のICカードの中には外部から与えられた電文を暗号化する機能を持ったものがある。この機能を利用して、第1から第4の実施形態で用いられている暗号化処理をキーカードC内で実施するよ

うにしても良い。

【0151】これにより、発行機プログラムの一部としてPC1内にある暗号プログラム自体を隠蔽することが出来るため、DES等の公開されている暗号ロジックだけでなく独自方式の暗号を使用できる。また、キーカードCにデータを投げ込むだけで暗号化結果が得られるため、暗号発行機プログラムの負荷も軽減される。

【0152】具体的には、図12、図15、図17、図19に示すPC1側における暗号化処理が、キーカードC内で行えるようにしている。

【0153】このキーカードCによるデータの暗号化処理を図25を用いて説明する。

【0154】この場合、キーカードC内には、指定コマンド番号に対するコマンド形式コマンド種が記憶され、この記憶されているコマンド形式（コマンド種）の1つが選択されている状態において、このコマンド種をPC1から供給される暗号化キーにより暗号化する暗号化プログラムを有している。

【0155】すなわち、発行コマンド電文である「暗号化するデータ列」のうち、コマンド形式の主たる部分をキーカードC内に格納しておき、PC1からはその機能番号（指定コマンド番号）と必要なパラメータ（実行パラメータ類）だけを渡すことで、キーカードC内でPC1で所望の発行コマンドを組み立てた上でさらにそれを暗号化してPC1へ出力することで、発行コマンドは完全に隠蔽される。この暗号化された発行コマンドは発行されるICカード4内で復号化・解釈されて実行されることについては、これまで示した例と変わりはない。

【0156】また、図25では、指定コマンド番号とパラメータ類を別々の矢印で示しているが、実際にカードに対して与える際には一コマンド化するようにしても良い。

【0157】このPC1側でのデータの暗号化（キーカードCによる）は、その時、発行対象となっているICカード4に対して送信されるコマンド電文を隠蔽するためのものなので、発行されるICカード4内で解釈できなければならないようになっている。このため、キーカードC側の暗号ロジックと発行されるICカード4側の復号ロジックは対応したものでなければならず、対象となるICカード4を発行するためには対応するキーカードCが必須となり、セキュリティをより高めることができる。

【0158】また、PC1側プログラムにコマンド電文は持たせないようにでき、PC1とキーカードCとの間に通信線があったとしても、コマンド電文は隠蔽されるようになっている。

【0159】また、図15、図17、図19に示すPC1側におけるキーを必要としない形の「乱数生成」処理があるが、これも論理的にはある固定の値のキーを使用している暗号化処理の一種と考えることができるため、

この乱数生成についてもキーカードCに委ねるようにしても良い。

【0160】このキーカードCによる乱数生成の処理を、図26を用いて説明する。

【0161】この場合、キーカードC内には、図25の構成にさらに指定キー番号に対応する複数の暗号化キーが記憶され、PC1からの指定キー番号に対応する暗号化キーが選択され、この選択された暗号化キーにより暗号化プログラムが暗号化を行うようになっている。

【0162】すなわち、キーカードC内には予め暗号化（乱数生成）のための暗号化キーが格納されており、この暗号化キーを使用して、発行コマンド電文である「暗号化するデータ列」のうち、コマンド形式の主たる部分をキーカードC内に格納しておき、PC1からはその機能番号（指定コマンド番号）と必要なパラメータ（実行パラメータ類）だけを渡すことで、キーカードC内でPC1で所望の発行コマンドを組み立てた上で、暗号（乱数）化してPC1へ出力する。

【0163】カード内の暗号化キーは複数格納することができ、暗号化処理の際にどの暗号化キーを使用するか指定も可能である。このキーの選択機能を利用して同一キーカードで複数システムに対応することが可能となる。キーカード内にシステム別に複数の暗号化キーを格納した場合、システム別の発行対象カードに適合したキーを指定する必要が発生し、セキュリティをより高めることができる。

【0164】この場合、隠蔽すべきデータは全てキーカードC内に格納され、発行機プログラムはキーカードCに対して発行されるカードに対して施したい処理とそれに必要な情報を示すだけで、発行処理が実現される。

【0165】なお、図26では、所望の指定コマンド番号とパラメータ類および指定キー番号を別々の矢印で示しているが、実際にキーカードCに対して与える際には一コマンド化するようにしても良い。

【0166】上述した図25、図26の例では、キーカードCと発行されるICカード4（＝適用システム）が対応づけられる旨の説明を加えたが、これをより強固にしてキーカードCによるセキュリティ確保の効果を高める方法について説明する。

【0167】図12、図15では、PC1側はコマンド電文暗号化用のキーをICカード4から取得し、図17、図19ではPC1側で乱数を生成しその値をそのまま、あるいはそれを種にして生成した新たな値を使用して暗号化を実施している。このキーや乱数の初期値を、予めキーカードCに格納された発行対象のICカード4に関連する情報をもとに生成させることで、事前のデータ交換を不要とする。これによって暗号化されたコマンド送信に先だってコマンド電文の暗号化に使用するデータを交換する方法に比べて、コマンド電文の秘匿に関するセキュリティは更に高くなる。

【0168】この方法の簡単な例を、図27を用いて説明する。

【0169】図25、図26の例では、発行コマンドをPC1（外部）から与えられるか番号によって指定されたキーにより暗号化しているが、このPC1からの入力無しに適用システム個別のキーデータをキーカードCと発行対象のICカード4に持ち合い、このキーを使用して、キーカードCでは発行コマンドを暗号化、発行対象のICカード4では受信した暗号化済み発行コマンドを復号化する。発行対象のICカード4のキーデータは、第1から第4の実施形態と同じく、製造時に適用システム別に格納する。

【0170】これにより、発行対象のICカード4は、一次発行処理において、一切の事前手続き無しに暗号化されたコマンド電文を受信してその内容を解釈してコマンド処理を実行できる。

【0171】ここまでのキーカードCの利用方法例は、図21、図22の機器構成を前提としてきたが、図28に示すように、PC1と一本の通信線Sで接続されキーカードCと発行対象のICカード4の両者が装着できるようなリーダライタ41を用いても良い。

【0172】また、図29に示すような、発行対象のICカード4が複数枚スタックされており、順次一枚ずつあるいは複数枚取り出されて発行処理が行なわれる様なリーダライタ50も、キーカードCの利用については、図28と同一ととらえることができる。リーダライタ50は通信線Sを介してPC1と接続されている。

【0173】このリーダライタ50は、未発行カードが複数枚スタックされている未発行カードスタック部51と、この未発行カードスタック部51から取出された1枚ずつの未発行カードを搬送し、搬送途中にて発行処理を行うカード搬送発行処理部52と、カード搬送発行処理部52により発行処理の行われたカードを収納する発行済みカード収納部53により構成されている。カード搬送発行処理部52には操作部54と動作状態表示部55とキーカードC用の差し込み口56が設けられている。

【0174】上記リーダライタ41、50においても、これまでに示したキーカードCの利用例は全て適応できるが、更にこの構成ならではの利用例について次に説明する。

【0175】図21、図22の構成では、各ICカード4と交換する電文は全てPC1を経由するが、図28、図29の構成では、ICカード4の電文をリーダライタ41、50内でクローズさせ外部に見えない形とすることができる。

【0176】一つの方法としては、図21の構成と同等の機能を、リーダライタ50の制御部がPC1の代役を務めることで実現し、リーダライタ41の制御部が独自にICカード4にアクセスするようにしても良い。

【0177】この実現例を、図30、図31、図32を用いて説明する。

【0178】すなわち、リーダライタ50は、リーダライタ50の全体を制御する制御部57、未発行カードスタック部51から発行済みカード収納部53へICカード4を搬送するカード搬送部58、カード搬送部58の途中に設けられる発行対象のICカード4に対してデータのリードライトを行う発行対象のICカード用のリーダライタ部59、キーカードC用の差し込み口56に差し込まれたキーカードCに対してデータのリードライトを行うキーカードC用のリーダライタ部60、操作部54、動作状態表示部55により構成されている。

【0179】このような構成において、カード発行処理時における、PC1、リーダライタ50の制御部57、キーカードC、ICカード4とのやりとりの例を、図310を用いて説明する。

【0180】すなわち、PC1はリーダライタ50の制御部57に対して通信線Sを通して動作指示を送り、リーダライタ50の制御部57が図12、図15、図17、図19の第1から第4の実施形態に示すICカード4とのやりとりを、図25、図26に示すキーカードCを利用した方法を含めて実施する形となる。

【0181】ここで、図25、図26中のコマンド形式の表は、図4に示したようなコマンドテンプレートの一覧である。

【0182】なお、リーダライタ50の制御部57に対するPC1からの動作指示は、ICカード4に対するコマンドと類似の電文による方法で実現できる。

【0183】このPC1からリーダライタ50に対する動作指示（コマンド）電文の例を図32に示す。図5に示したICカード4に対するコマンド電文に対してコマンドコードが動作種別指示コードに変わっただけのものである。

【0184】このコマンド電文は、リーダライタ50の表示部55への表示内容、ICカード4の搬送、リーダライタ50の動作状態の取得等を含むリーダライタ50本体動作全体に関する動作を指示するためのものである。その動作指示の一つとしてカード発行処理に関する動作指示があり、この場合動作種別指示コードには、キーカードCの（図25、図26のいずれを適用するかといった）使用方法を含めた意味内容のコード割り付けが行われる。動作種別指示コードにキーカードCの使用方法まで含んだ場合、実行パラメータの中にカードに対するコマンドの種別を入れ、その発行処理に必要な作成するファイルの名前や大きさといった情報を処理用データとして示すようにしても良い。

【0185】この様な動作指示（コマンド）電文を使用して、図30の様な構成の機器でPC1がリーダライタ50を制御して、図20のキーカードCから暗号化されたコマンド電文を取得して発行対象カードに送るのと同

様の処理を実施した際の動作を図 31 に示す。

【0186】すなわち、PC1 から動作指示（コマンド）電文を受信した、リーダライタ 50 の制御部 57 は受け取った指示内容に従ってキーカード C と発行対象の IC カード 4 をアクセスして発行処理を実施し、その実行結果を動作結果通知電文として PC1 に対して返送する。

【0187】たとえば、制御部 57 は PC1 から受け取ったリーダライタ動作指示コマンドを解釈し、このコマンドによりキーカード向けのコマンド電文を生成し、このコマンド電文を用いてキーカード C に対する処理（要求コマンド種別とパラメータをキーカード C へ出力）を行い、この処理によりキーカード C から得られる暗号化済みコマンド電文を用いて発行対象の IC カード 4 に対する処理（はつこう一美コマンド電文を IC カード 4 に出力）を行い、この処理により IC カード 4 から得られるコマンド実行結果に基づいて PC1 向けのレスポンス電文を生成し、この生成したレスポンス電文をリーダライタ動作結果通知として PC1 へ出力する。

【0188】もちろん、図 23 に示すような発行システム起動時のキーカード処理も、図 31 の様なカード発行処理以前に実施されるようになっている。

【0189】なお、以上全ての例は IC カード発行機システムに限らず、IC カード 4 に対するコマンド電文を隠蔽したい場合、全てに適用できる。

【0190】特に、キーカード C を使用方法については、近年登場してきている個人が保有する通常の取引用カードとは別にセキュリティアクセス管理カードを内蔵するような電子マネーのチャージ端末等の、セキュリティアクセス管理カードを発行機システムでのキーカード C と同様に利用することで同等の機能が実現できる。

【0191】この場合、発行機システムでは製造時に格納していたカードあるいはシステム個別のデータは、取引用のカードが利用者個人の手に渡るまでの間に格納されればよい。

【0192】上記したように、発行対象の IC カードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関する IC カードのセキュリティを向上させることができる。

【0193】また、そのコマンド電文の暗号化に関する PC 側の処理に使用するデータ類を発行機システムには一般的なキーカードに格納することで、そのセキュリティをより向上させることができる。

【0194】また、PC 側での暗・復号処理自体をキーカード内で実施することで、そのセキュリティを更に向上させることができる。

【0195】また、この様なキーカードを、キーカードと発行対象のカードの両者を同一筐体内に保持する様な

形式のリーダライタで扱う場合、キーカードから出力されるデータをリーダライタ内でクローズして使用することで、そのセキュリティは更に向上する。

【0196】

【発明の効果】以上詳述したように、この発明によれば、発行対象カードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関する IC カードのセキュリティを向上させることができる。

【0197】また、この発明によれば、コマンド電文の暗号化に関する端末機側の処理に使用するデータ類を発行機システムには一般的なキーカードに格納することで、そのセキュリティをより向上させることができる。

【0198】また、この発明によれば、端末機側での暗・復号処理自体をキーカード内で実施することで、そのセキュリティを更に向上させることができる。

【0199】また、この発明によれば、この様なキーカードを、キーカードと発行対象のカードの両者を同一筐体内に保持する様な形式のリーダライタで扱う場合、キーカードから出力されるデータをリーダライタ内でクローズして使用することで、そのセキュリティは更に向上させることができる。

【図面の簡単な説明】

【図 1】この発明の IC カード発行システムの構成を示すブロック図。

【図 2】IC カードの内部構成を示すブロック図。

【図 3】PC の機能を説明するための図。

【図 4】発行コマンドテンプレートの構成を説明するための図。

【図 5】IC カード 4 に対するコマンド電文の一般形の例を示す図。

【図 6】暗号化済みのコマンド電文の例を示す図。

【図 7】IC カードの EEPROM 内に格納するデータのフォルダ、ファイルのツリー構造を説明するための図。

【図 8】アプリケーションフォルダの管理情報の例を示す図。

【図 9】キーファイルの管理情報の例を示す図。

【図 10】データファイルの管理情報の例を示す図。

【図 11】第 2 の実施形態における IC カードの発行処理を説明するためのフローチャート。

【図 12】第 2 の実施形態における IC カードの発行処理を説明するための図。

【図 13】第 3 の実施形態における IC カードの発行処理を説明するためのフローチャート。

【図 14】第 3 の実施形態における IC カードの発行処理を説明するためのフローチャート。

【図 15】第 3 の実施形態における IC カードの発行処

10

20

30

40

50

理を説明するための図。

【図 16】第 4 の実施形態における IC カードの発行処理を説明するためのフローチャート。

【図 17】第 4 の実施形態における IC カードの発行処理を説明するための図。

【図 18】第 4 の実施形態における IC カードの発行処理を説明するためのフローチャート。

【図 19】第 4 の実施形態における IC カードの発行処理を説明するための図。

【図 20】暗号化用キーデータも含んだキーカードの記憶内容示す図。

【図 21】キーカードを用いる IC カード発行システムの構成を示すブロック図。

【図 22】キーカードを用いる IC カード発行システムの構成を示す図。

【図 23】キーカードを用いた IC カードの発行処理を説明するためのフローチャート。

【図 24】発行機プログラム起動処理のコードの分割記憶を説明するための図。

【図 25】キーカードによるデータの暗号化処理を説明 20 するための図。

【図 26】キーカードによる乱数生成の処理とデータの＊

＊暗号化処理を説明するための図。

【図 27】キーカードと PC と IC カードのデータのやり取りを説明するための図。

【図 28】IC カード発行システムの構成を示す図。

【図 29】IC カード発行システムの構成を示す図。

【図 30】IC カード発行システムの構成を示すブロック図。

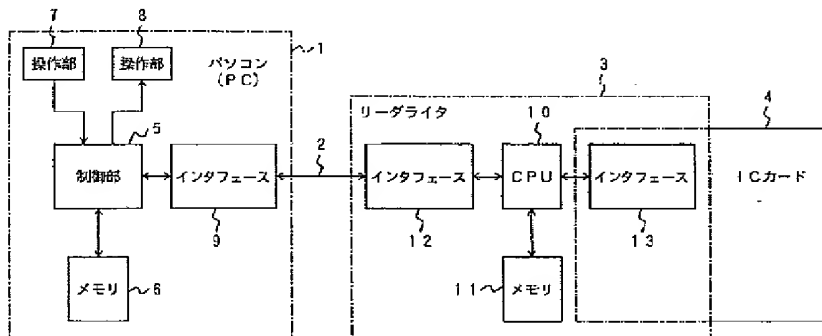
【図 31】PC とリーダライタとキーカードと IC カードのデータのやり取りを説明するための図。

【図 32】PC からリーダライタに対するコマンド電文の例を示す図。

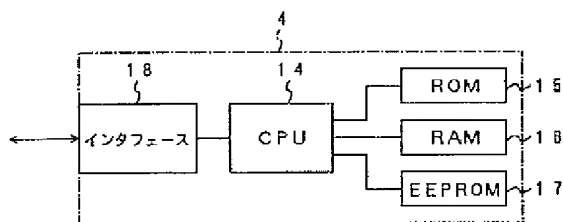
【符号の説明】

- 1…PC
- 2…通信ライン
- 3…リーダライタ
- 4…IC カード
- 5…制御部
- 6…メモリ
- 14…CPU
- 15…ROM
- 17…EEPROM
- C…キーカード

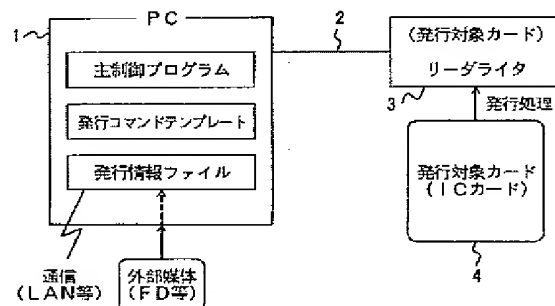
【図 1】



【図 2】



【図 3】



【図4】

フォルダファイル生成コマンドテンプレート

フォルダ/ファイル生成コマンドコード	フォルダ/ファイル指定	フォルダ/ファイル管理情報
キー設定コマンドテンプレート		
キー設定コマンドコード	キーファイル(I D)指定	キーデータ長 実キーデータ部
コマンド処理内容表示部分		
コマンドコード	実行パラメータ	処理用データ

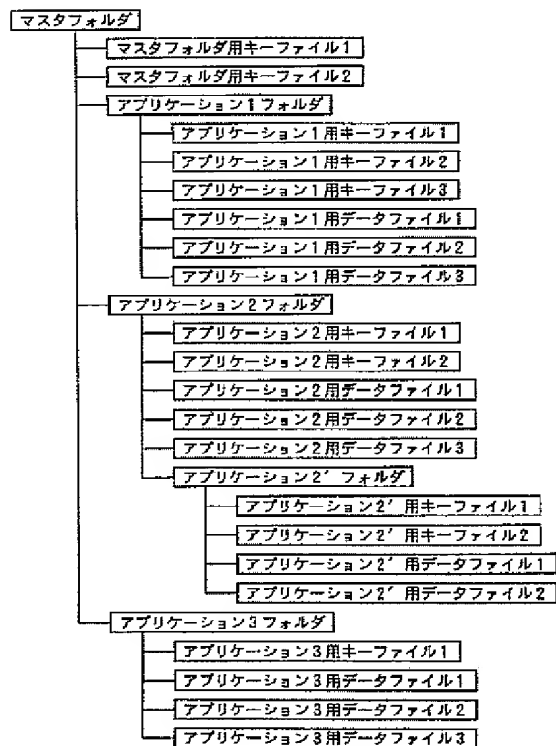
【図5】

2 1	2 2	2 3	2 4	2 5	2 6
先頭符号	送信電文長	コマンドコード	実行パラメータ	処理用データ	末尾符号

【図6】

2 1	2 2	2 7	2 6
先頭符号	送信電文長	符号化されたコマンド処理内容表示部	末尾符号

【図7】



一次発行処理で生成されるファイル構造の一例

【図8】

フォルダ名称	フォルダサイズ	上位フォルダ	参照アクセス権	変更アクセス権
--------	---------	--------	---------	---------

アプリケーションフォルダ管理情報

【図9】

ファイルID	キーデータ長	キー種別	参照アクセス権	変更アクセス権
--------	--------	------	---------	---------

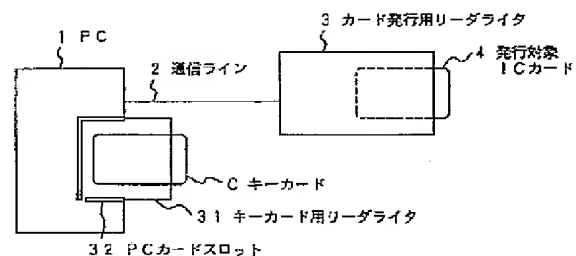
キーデータファイル管理情報

【図10】

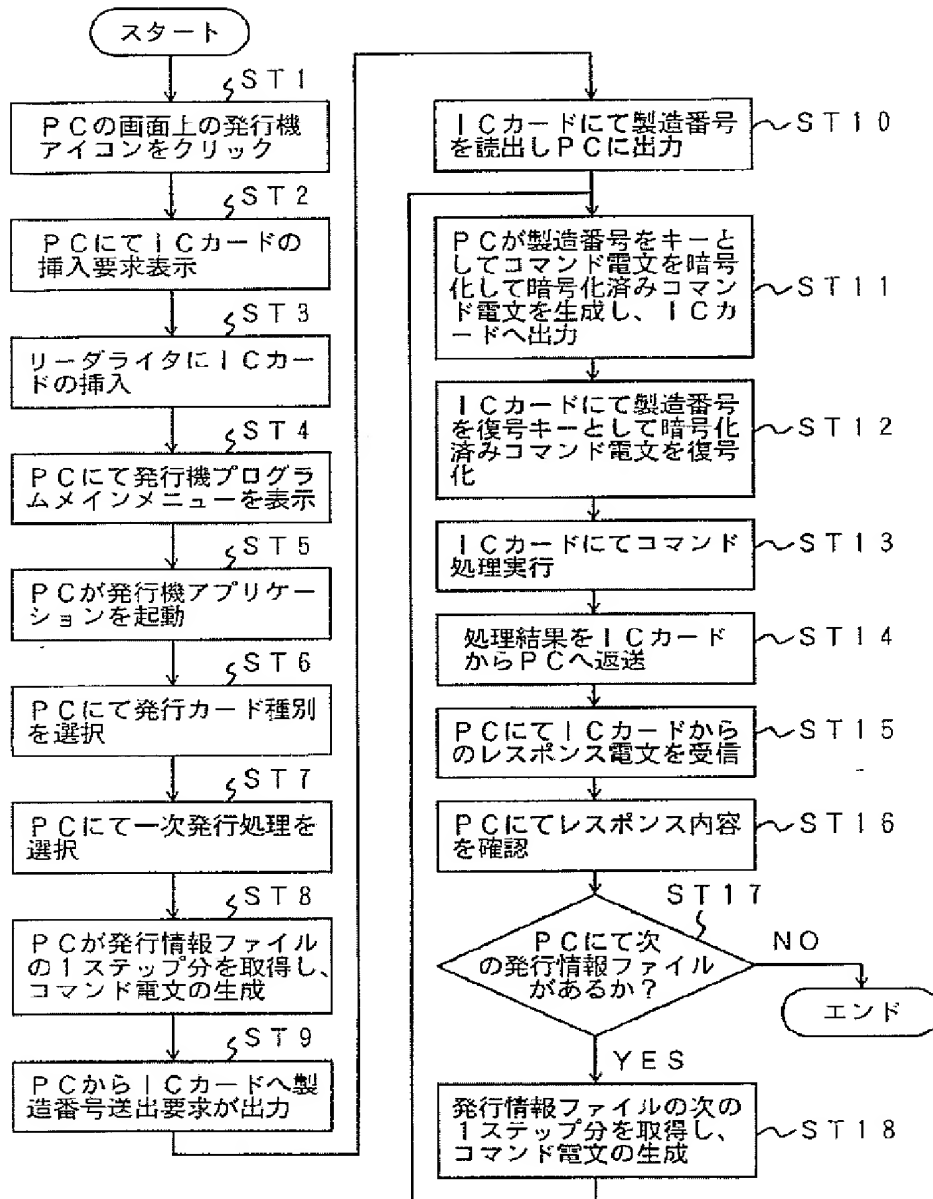
ファイルID	ファイルサイズ	ファイル種別	参照アクセス権	変更アクセス権
--------	---------	--------	---------	---------

アプリ用データファイル管理情報

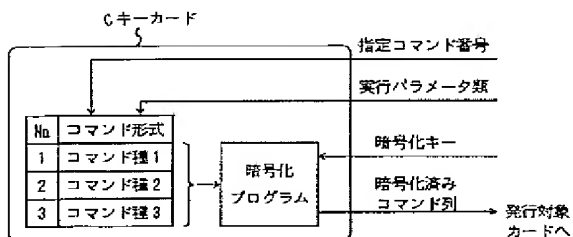
【図22】



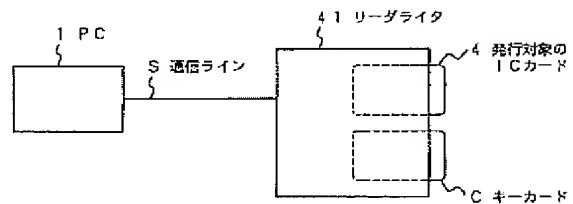
【図11】



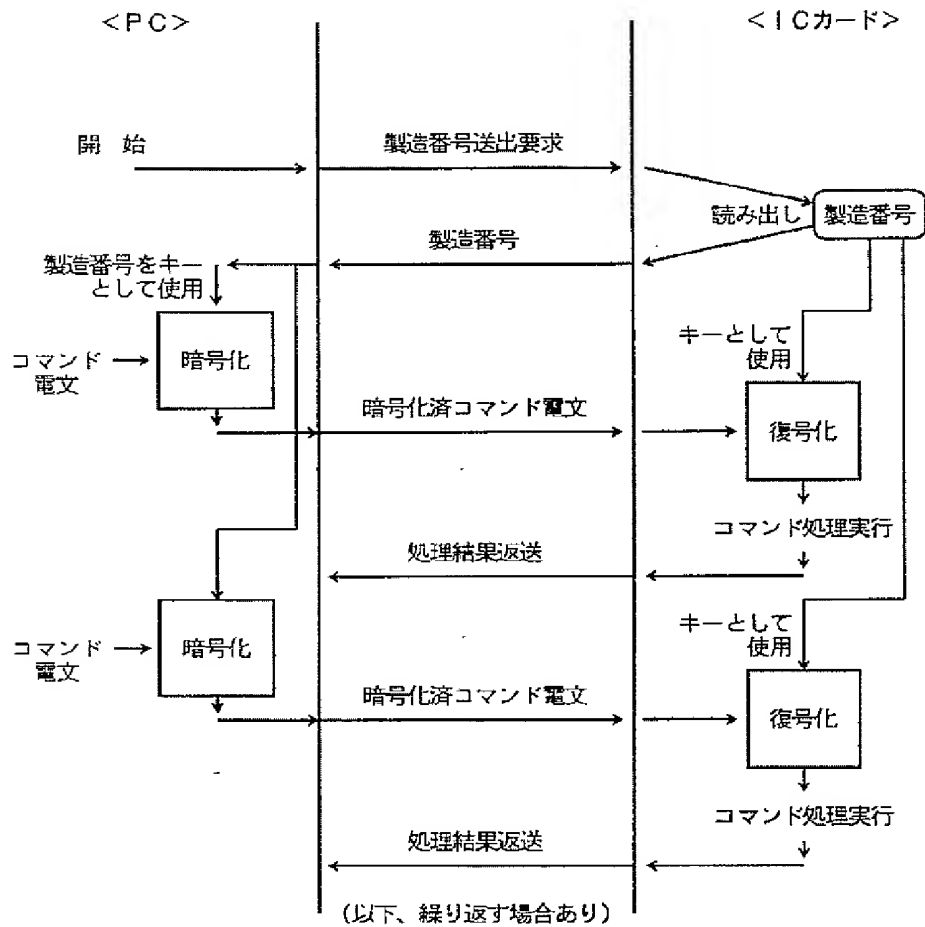
【図25】



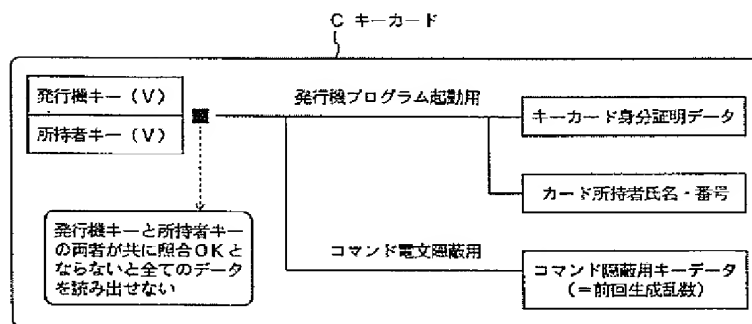
【図28】



【図 12】



【図 20】

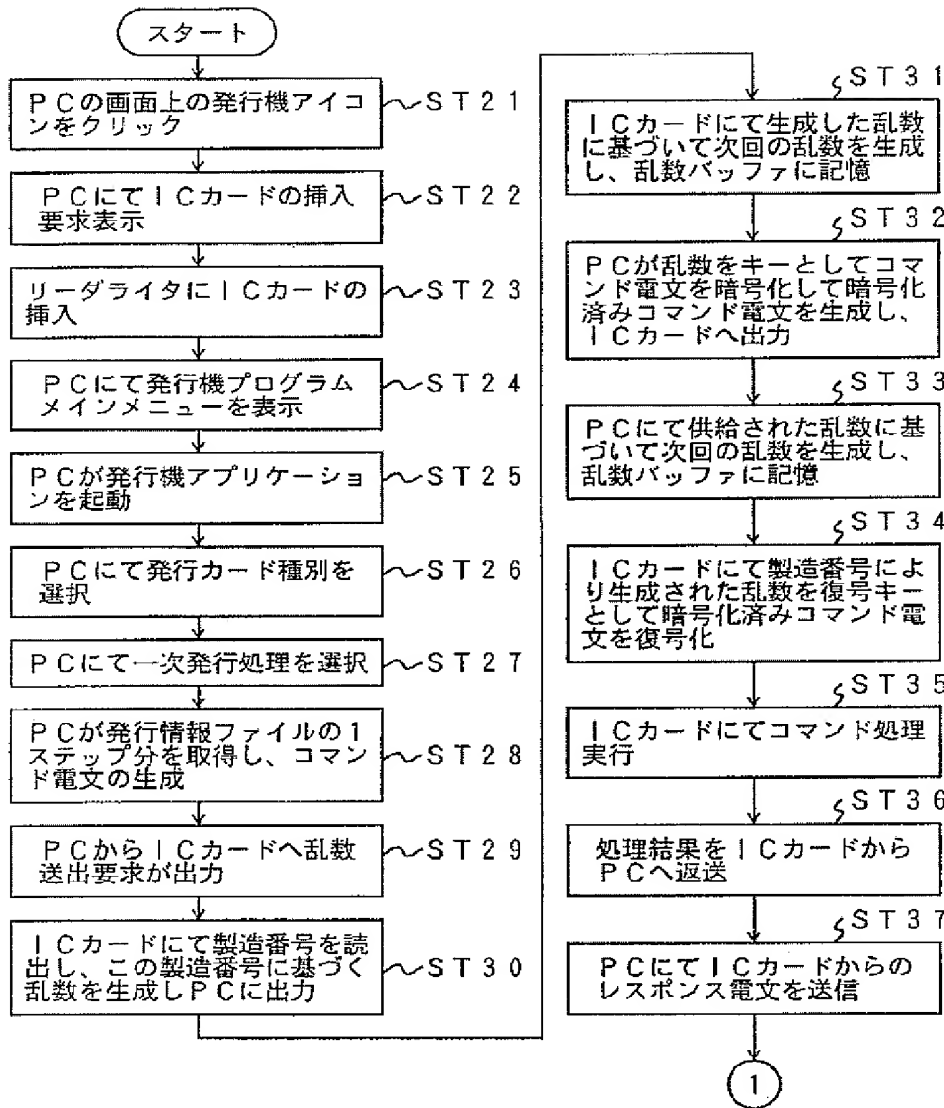


(V) : カード内での照合用データであることを示す

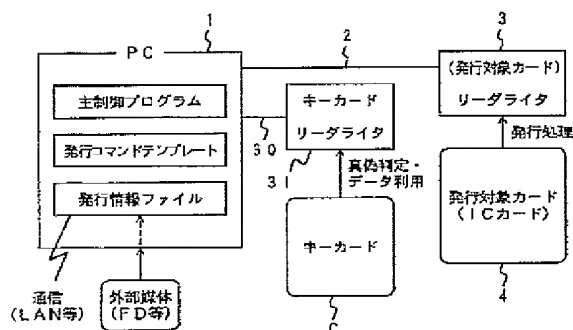
【図 32】

先頭符号	送信電文長	動作識別指示コード	実行パラメータ	処理用データ	末尾符号
------	-------	-----------	---------	--------	------

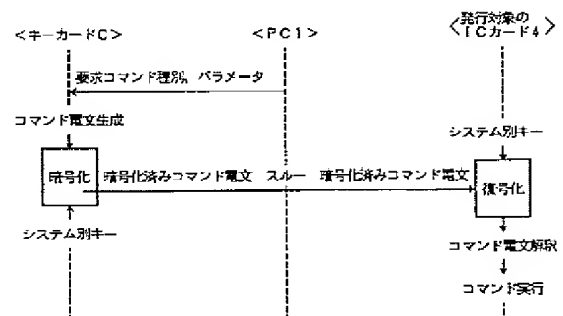
【図13】



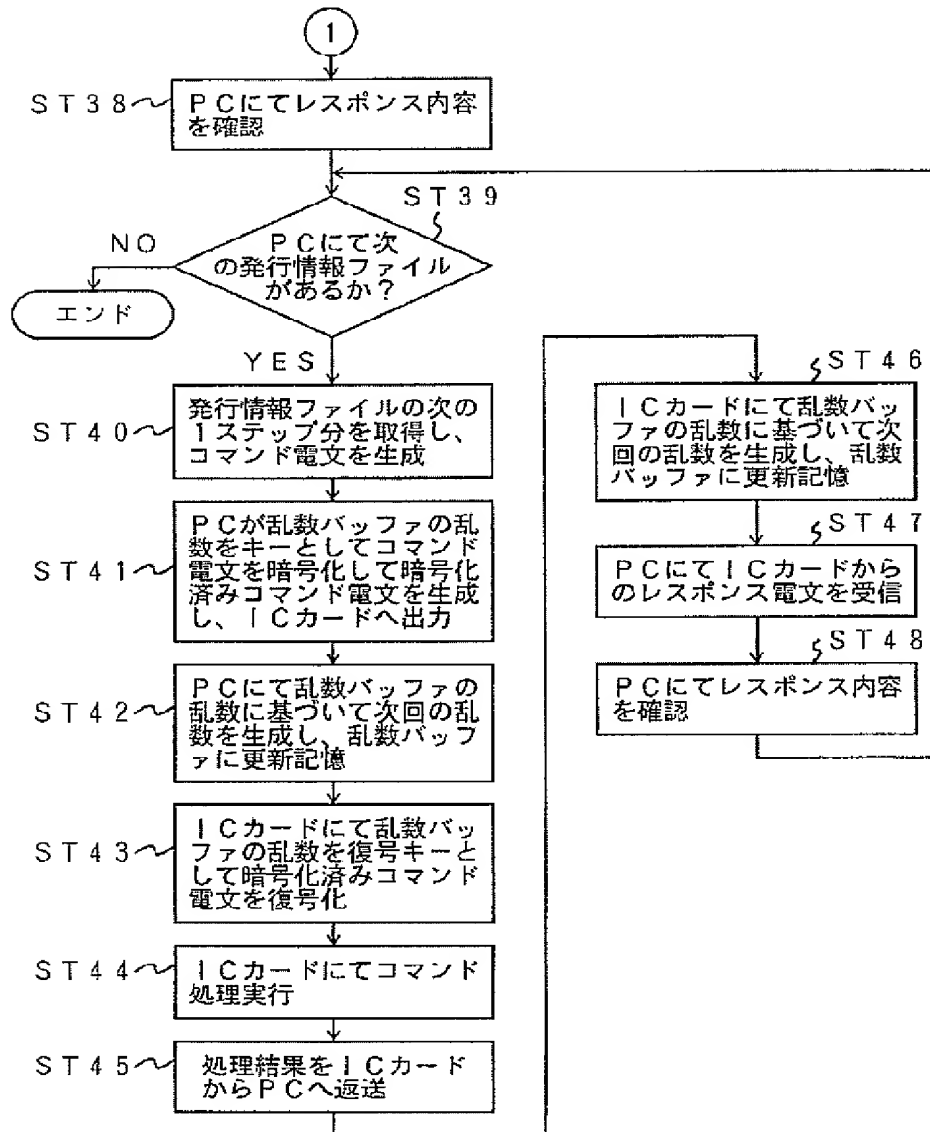
【図21】



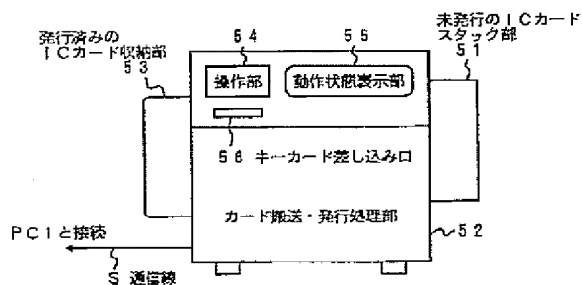
【図27】



【図14】



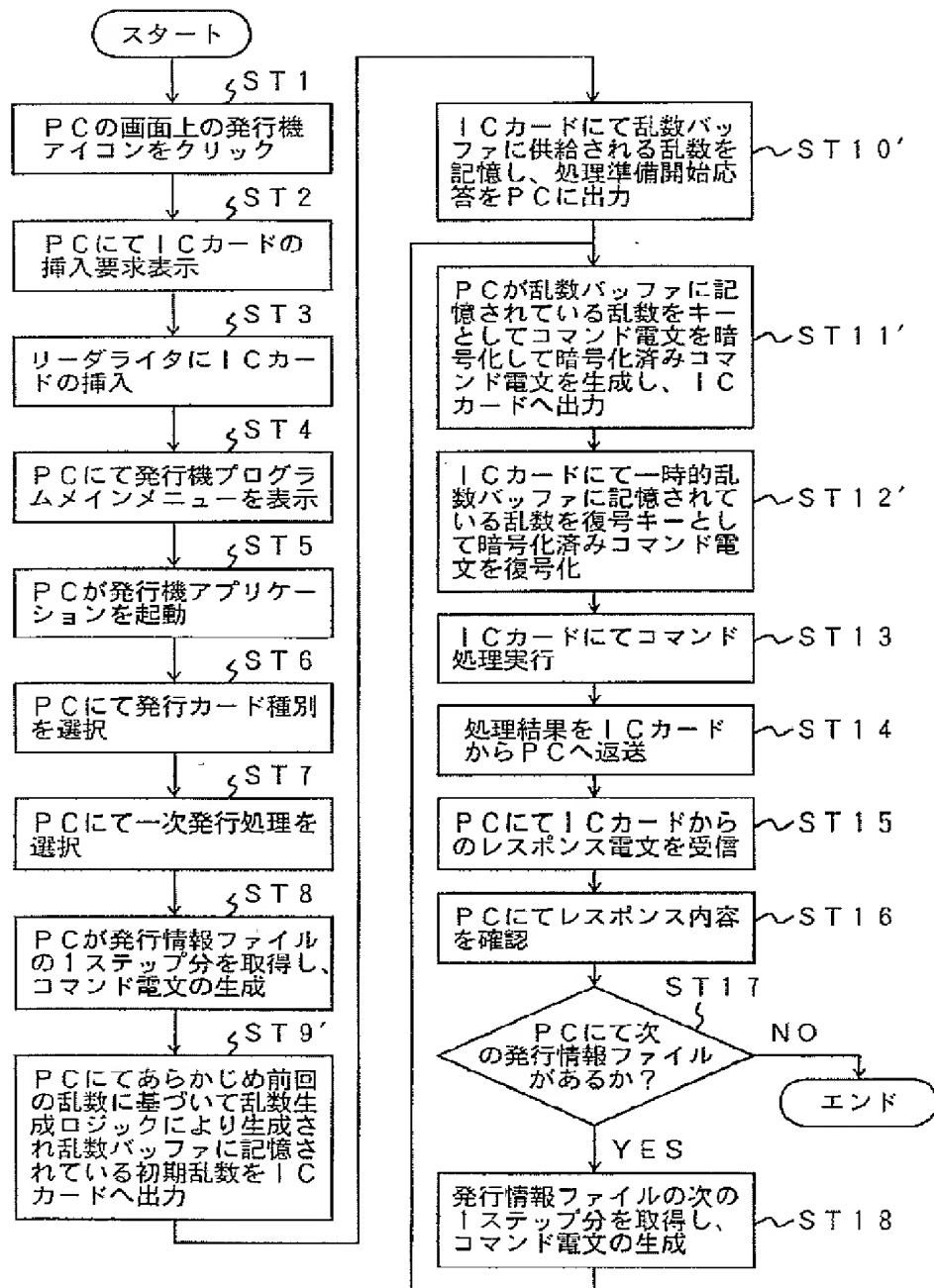
【図29】



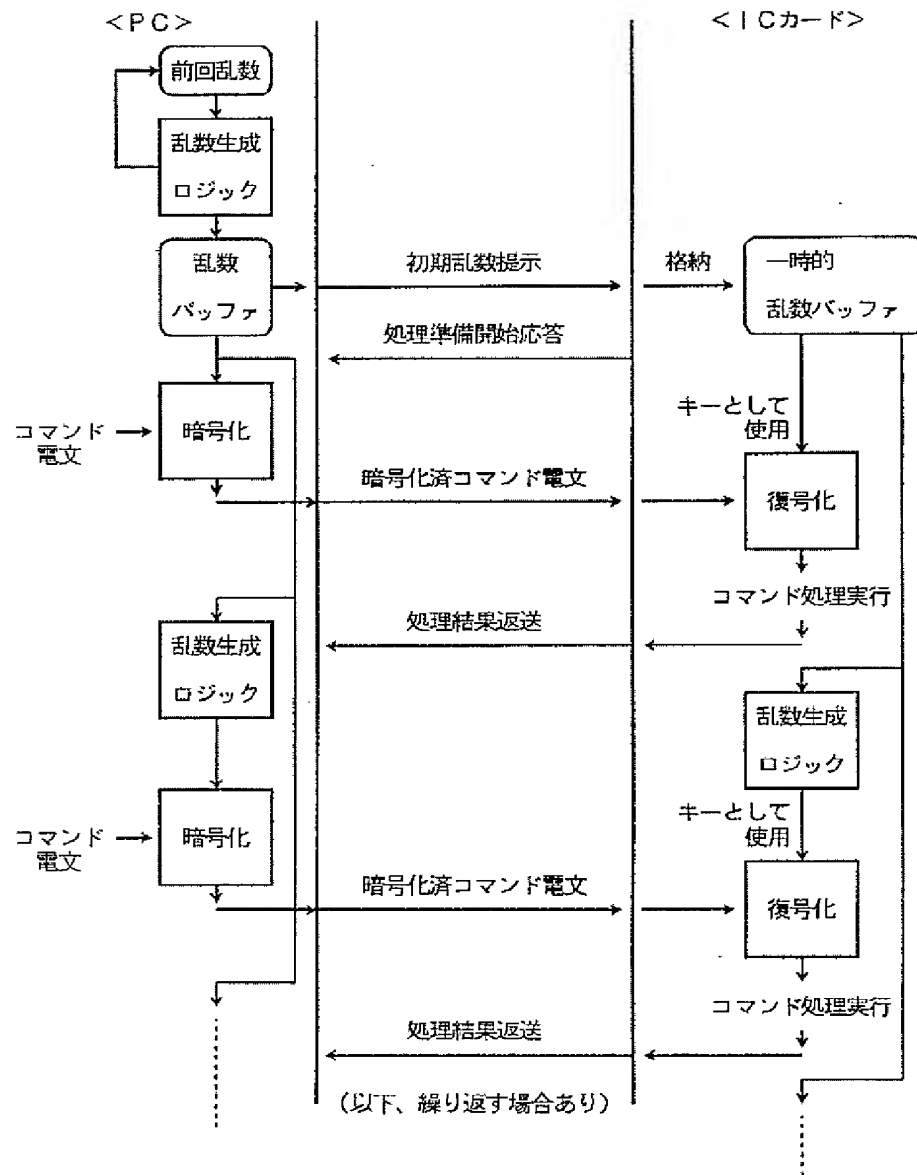
The sequence diagram illustrates the interaction between a PC and an IC Card:

- PC Side:**
 - Starts with "開始" (Start).
 - Sends "乱数送出要求" (Random number output request) to the IC Card.
 - Receives "生成乱数" (Generated random number) from the IC Card.
 - Uses the received random number as a key ("生成乱数をキーとして使用").
 - Processes a "コマンド電文" (Command message) through "暗号化" (Encryption).
 - Sends "暗号化済コマンド電文" (Encrypted command message) to the IC Card.
 - Receives "処理結果返送" (Return of processing result) from the IC Card.
 - Generates its own random number ("乱数生成 ロジック") and stores it in a buffer ("次回乱数バッファ").
 - Processes another "コマンド電文" through "暗号化".
 - Sends "暗号化済コマンド電文" to the IC Card.
 - Receives "処理結果返送" from the IC Card.
 - The process can repeat ("以下、繰り返す場合あり").
- IC Card Side:**
 - Initializes with "製造番号" (Manufacture number).
 - Responds to the PC's request by performing "乱数生成 ロジック" (Random number generation logic) and sending "出力乱数 バッファ" (Output random number buffer).
 - Uses the received random number as a key ("キーとして使用").
 - Performs "復号化" (Decryption) on the received command message.
 - Executes "コマンド処理実行" (Command processing execution).
 - Generates its own random number ("乱数生成 ロジック") and stores it in a buffer ("次回乱数バッファ").
 - Uses the received random number as a key ("キーとして使用").
 - Performs "復号化" (Decryption) on the received command message.
 - Executes "コマンド処理実行" (Command processing execution).
 - The process can repeat ("以下、繰り返す場合あり").

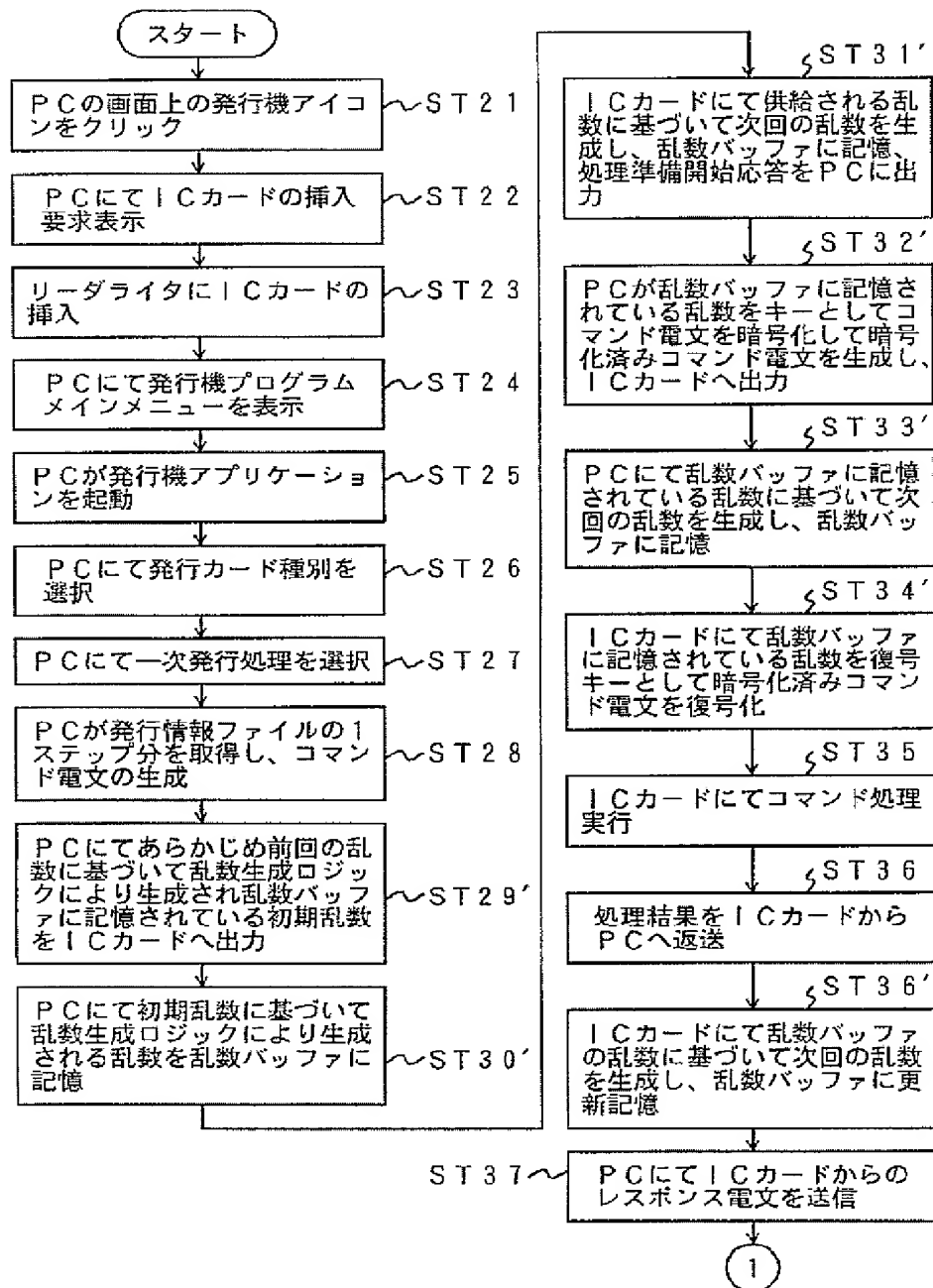
【図16】



【図 17】



【図18】



The flowchart illustrates the interaction between a PC and an IC card for random number generation and command processing. The process is divided into two main sections: PC operations and IC card operations, separated by a vertical line.

PC Operations:

- Initial State:** The PC starts with a "前回乱数" (Previous Random Number) stored in a box.
- Initial Random Number Generation:** The "乱数生成 ロジック" (Random Number Generation Logic) block generates a new random number, which is then stored in the "前回乱数 バッファ" (Previous Random Number Buffer) block.
- Command Processing:** When a "コマンド電文" (Command Data) is received, it is sent to the "暗号化" (Encryption) block. The encryption process uses the random number from the "前回乱数 バッファ" block as a key.
- Result Return:** After encryption, the "暗号化済コマンド電文" (Encrypted Command Data) is sent back to the IC card via "処理結果返送" (Return of Processing Result).
- Next Step:** The PC then generates another random number and stores it in the "前回乱数 バッファ" block for the next command.

IC Card Operations:

- Initial State:** The IC card starts with a "前回乱数" (Previous Random Number) stored in a box.
- Initial Random Number Generation:** The "乱数生成 ロジック" (Random Number Generation Logic) block generates a new random number, which is then stored in the "前回乱数 バッファ" (Previous Random Number Buffer) block.
- Key Usage:** The random number from the "前回乱数 バッファ" block is used as a "キーとして使用" (Used as a Key) for the "復号化" (Decryption) block.
- Command Processing:** When an "暗号化済コマンド電文" (Encrypted Command Data) is received from the PC, it is sent to the "復号化" (Decryption) block.
- Result Return:** After decryption, the "コマンド処理実行" (Command Processing Execution) block performs the command, and the result is sent back to the PC via "処理結果返送" (Return of Processing Result).
- Next Step:** The IC card then generates another random number and stores it in the "前回乱数 バッファ" block for the next command.

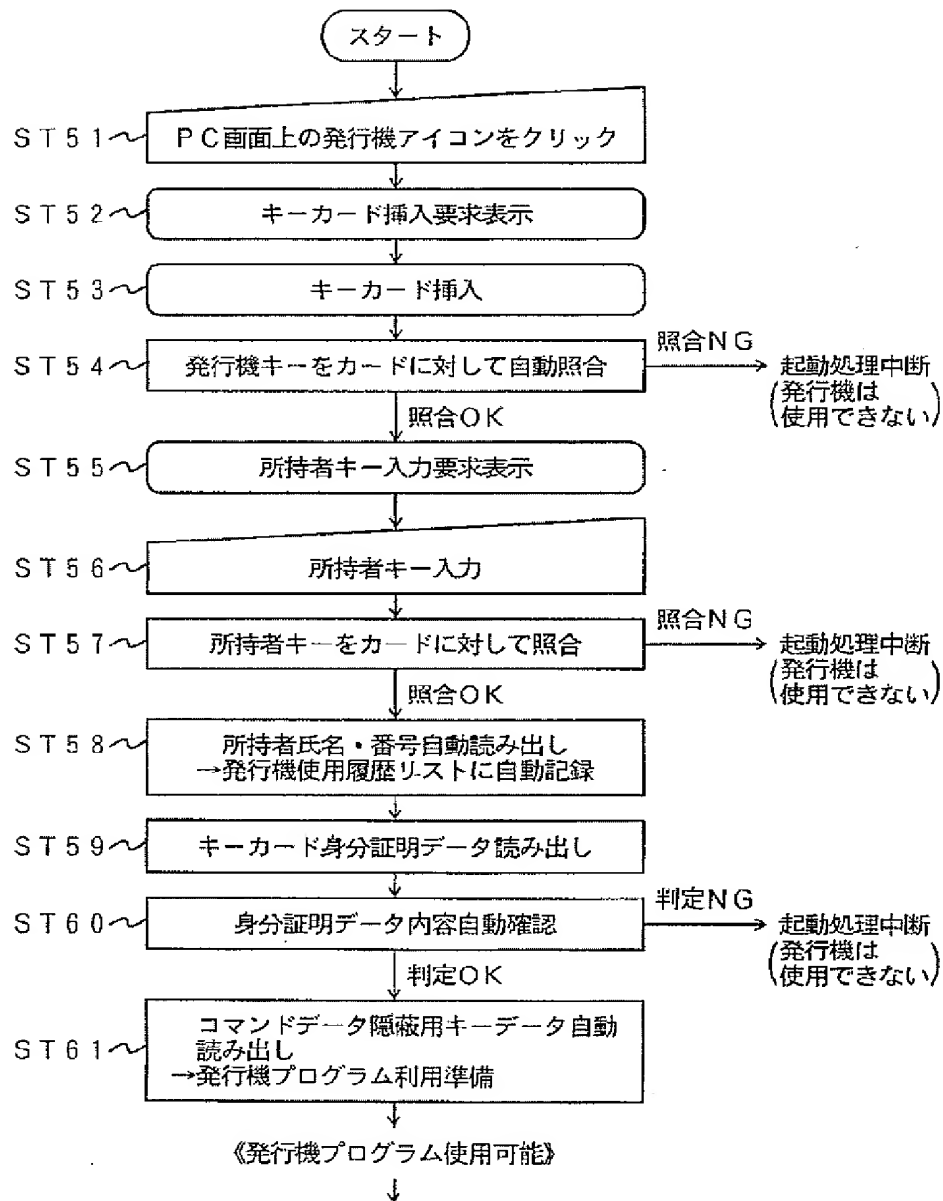
Communication and Flow:

- 初期乱数提示** (Initial Random Number Prompt) is sent from the PC to the IC card.
- 処理開始準備完了** (Processing Start Preparation Complete) is sent from the IC card to the PC.
- The flow repeats for multiple commands, with the PC always sending the "暗号化済コマンド電文" and the IC card always returning the "処理結果返送".
- A dashed line at the bottom indicates that the process can loop back, with a note: "(以下、繰り返す場合あり)" (Below, repetition is possible).

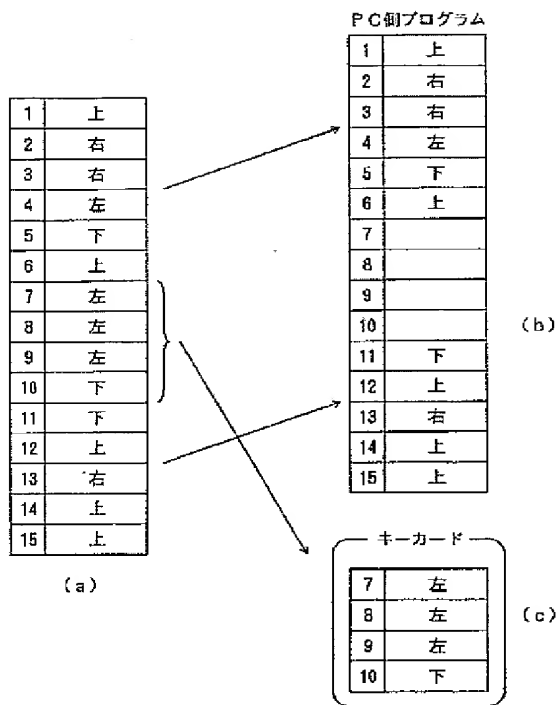
Additional Notes:

- A note on the left side of the PC section states: "この繰り返しの最後の乱数値を前回乱数に格納する方法もあり" (There is also a method to store the random number value at the end of this repetition in the previous random number).
- A note on the right side of the IC card section, enclosed in a dashed box, says: "修整" (Revision/Correction).

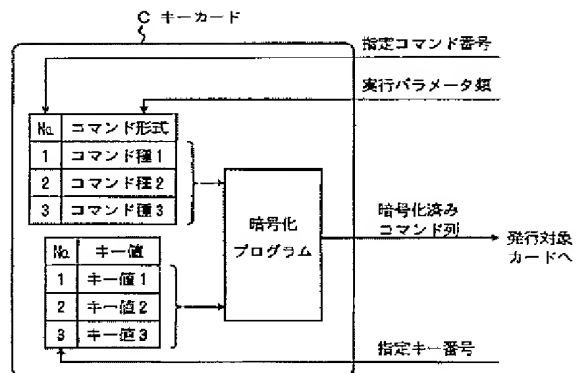
【図 23】



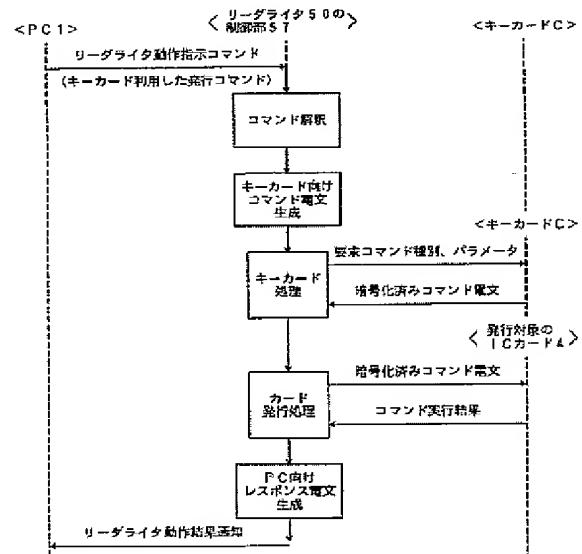
【図 24】



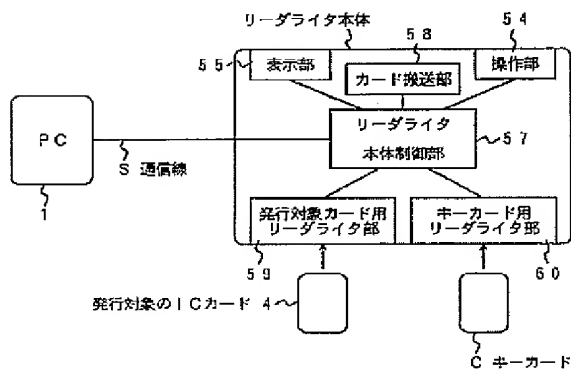
【図 26】



【図 31】



【図 30】



フロントページの続き

(51) Int. Cl.⁷
H04L 9/36

識別記号

FI
H04L 9/00

テーマコード(参考)

685

